

ALLNET ALL39x

Carrier Class DD-WRT

Benutzerhandbuch

1. Intro

1.1. Willkommen

Vielen Dank dass Sie sich für die professionellen Outdoor Produkte von ALLNET entschieden haben. Diese Geräte erlauben es Ihnen, WLAN-Verbindungen in vielfältiger Weise für den Aufbau leistungsfähiger Netzinfrastrukturen im Außenbereich zu nutzen. Die Allnet Outdoor Router verwenden die OpenSource-Firmware DD-WRT®, einer der leistungsfähigsten linuxbasierten Firmwares am Markt.

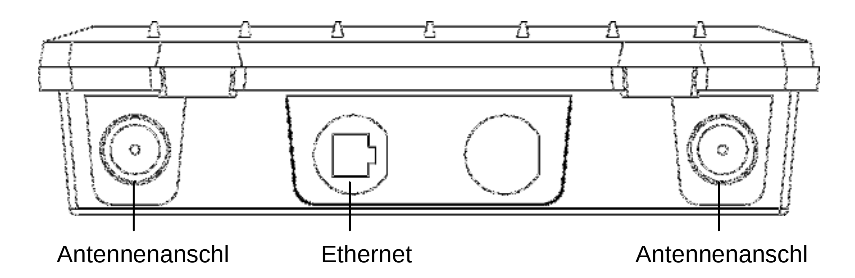
Diese Kurzanleitung bietet Ihnen einen ersten Überblick über die Funktionen und erläutert anhand von Beispielen die Gerätekonfiguration für typische Anwendungsfälle. Weiterführende Informationen finden Sie unter http://www.dd-wrt.com/wiki/.

1.2. Verpackungsinhalt

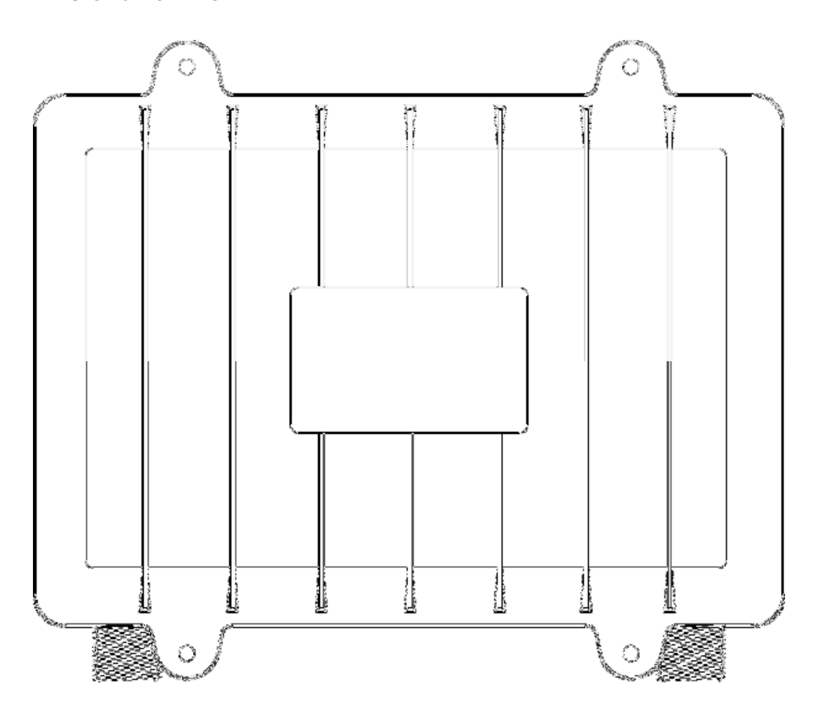
- Router
- Masthalterung + Montagematerial
- Kurzbeschreibung

1.3. Grundlegende Geräteinformationen

Ansicht von unten



Ansicht von vorn



1.4. Gerätekonfiguration

Ab Werk ist der Router als Bridge konfiguriert, d.h. alle Netzwerkinterfaces (Ethernet & WLAN) kommunizieren miteinander über die interne Bridge. Dadurch ist der Router sofort einsatzbereit und kann mit wenigen Änderungen gegenüber der Werkskonfiguration in Betrieb genommen werden.

1.4.1. Werkseinstellungen

Da auf dem Gerät per default alle Interfaces der Bridge zugeordnet sind, gilt für alle die gleiche IP-Konfiguration:

IP-Adresse	192.168.1.1
Netzmaske	255.255.255.0
DHCP-Server	aktiv
DHCP-Range	192.168.1.100 - 150

Die WLAN-Interfaces sind standardmäßig aktiviert und senden die SSID „dd-wrt“ aus. Aus Sicherheitsgründen sollten bei der Erstinbetriebnahme nicht benötigte WLAN-Interfaces deaktiviert oder mit einer Verschlüsselung mit entsprechend sicherer Passphrase versehen werden.

1.4.2. Inbetriebnahme

Der Router wird über PoE (Power over Ethernet) mit Strom versorgt. Dabei sind Eingangsspannungen zwischen 9 und 48V DC möglich. Nach dem Aktivieren der Spannungsversorgung ist der Router unter der IP-Adresse 192.168.1.1 über die integrierte Ethernet-Schnittstelle per Telnet oder WebBrowser ansprechbar. Standardmäßig ist der DHCP-Server auf der Bridge aktiviert, sodass ein angeschlossener PC automatisch eine passende Adresse zugewiesen bekommt, wenn die entsprechende Ethernet-Adresse auf DHCP konfiguriert ist.

Da alle Einstellungen über das Webinterface vorgenommen werden können, wird in dieser Anleitung nur die Konfiguration über dieses betrachtet.

2. Konfiguration über das Webinterface

Der Router verfügt über einen integrierten WebServer, mit dessen Hilfe ein komfortables und übersichtlich strukturiertes Webinterface bereitgestellt wird. Dieses Webinterface erlaubt die Konfiguration, Administration sowie eine Statusprüfung des Routers.

Beim ersten Zugriff ist es erforderlich, die Standardkennung für den Administrationszugriff „root“ / „admin“ zu ändern. Die Statusseite ist vom internen Netz des Routers auch ohne Eingabe der Administratorkennung zugänglich, dies kann aber deaktiviert werden.

Das Webinterface wurde mit den folgenden Browsern erfolgreich getestet:
- Internet Explorer 6.x und neuer
- Firefox 2.x und neuer
- Safari 2.x und neuer

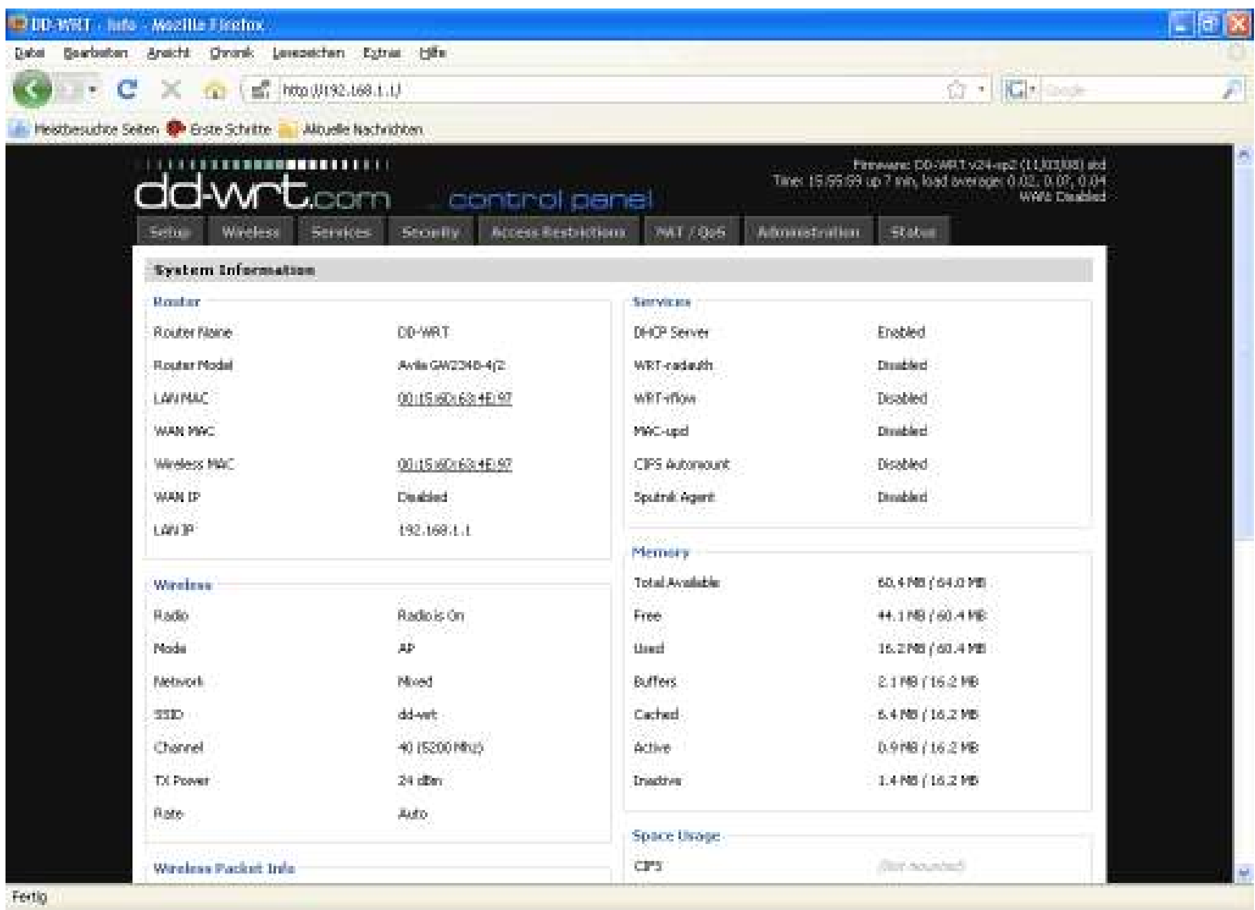
2.1. Vorbereitungen

Schließen Sie den Router wie unter 1.4.2. beschrieben an eine PoE Spannungsquelle an und verbinden Sie die Ethernet Schnittstelle des Rechners, den Sie zur Konfiguration verwenden, mit dem der Ethernet-Schnittstelle des Routers. Konfigurieren Sie die Ethernet-Schnittstelle des Konfigurationsrechners entweder auf DHCP oder setzen Sie eine feste IP-Adresse aus dem 192.168.1er Netz (z.B. 192.168.1.10), nicht aber 192.168.1.1. Wenn Sie die Schnittstelle auf DHCP gesetzt haben, werden IP-Adresse, Netzmaske und Gateway-Adresse vom Router zugewiesen.

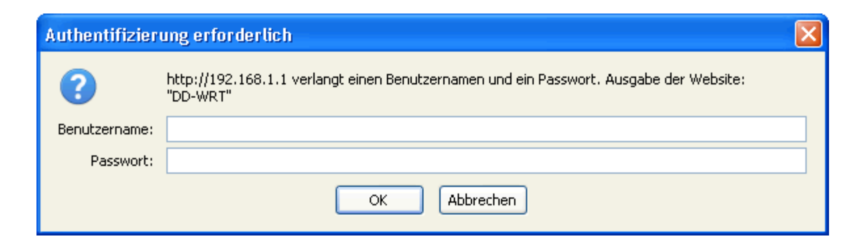
Nachdem der Router sein System geladen hat, ist er über die Netzwerkschnittstelle ansprechbar, dies lässt sich am einfachsten über einen Ping auf die Adresse 192.168.1.1 prüfen.

2.2. Zugriff auf das Webinterface

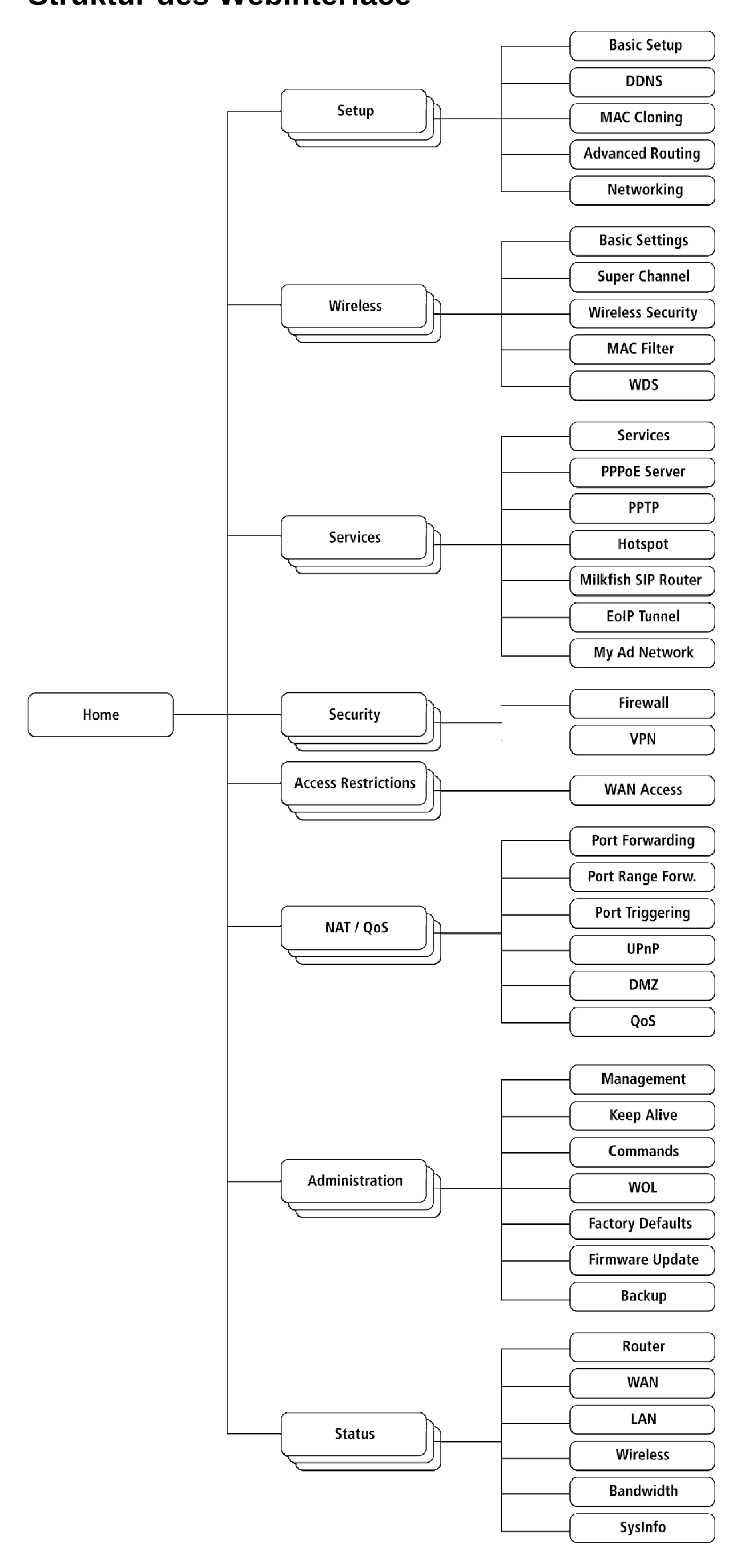
Verwenden Sie einen der unter 2. aufgeführten Browser und geben Sie in der Adresszeile http://192.168.1.1 ein. Wenn alle Einstellungen korrekt sind, erscheint die folgende Statusseite mit den grundlegenden Betriebsinformationen des Routers:



Wenn Sie einen der Tabs für ein Administrationsmenü anklicken, werden Sie aufgefordert, die von Ihnen initial gesetzte Benutzerkennung einzugeben:

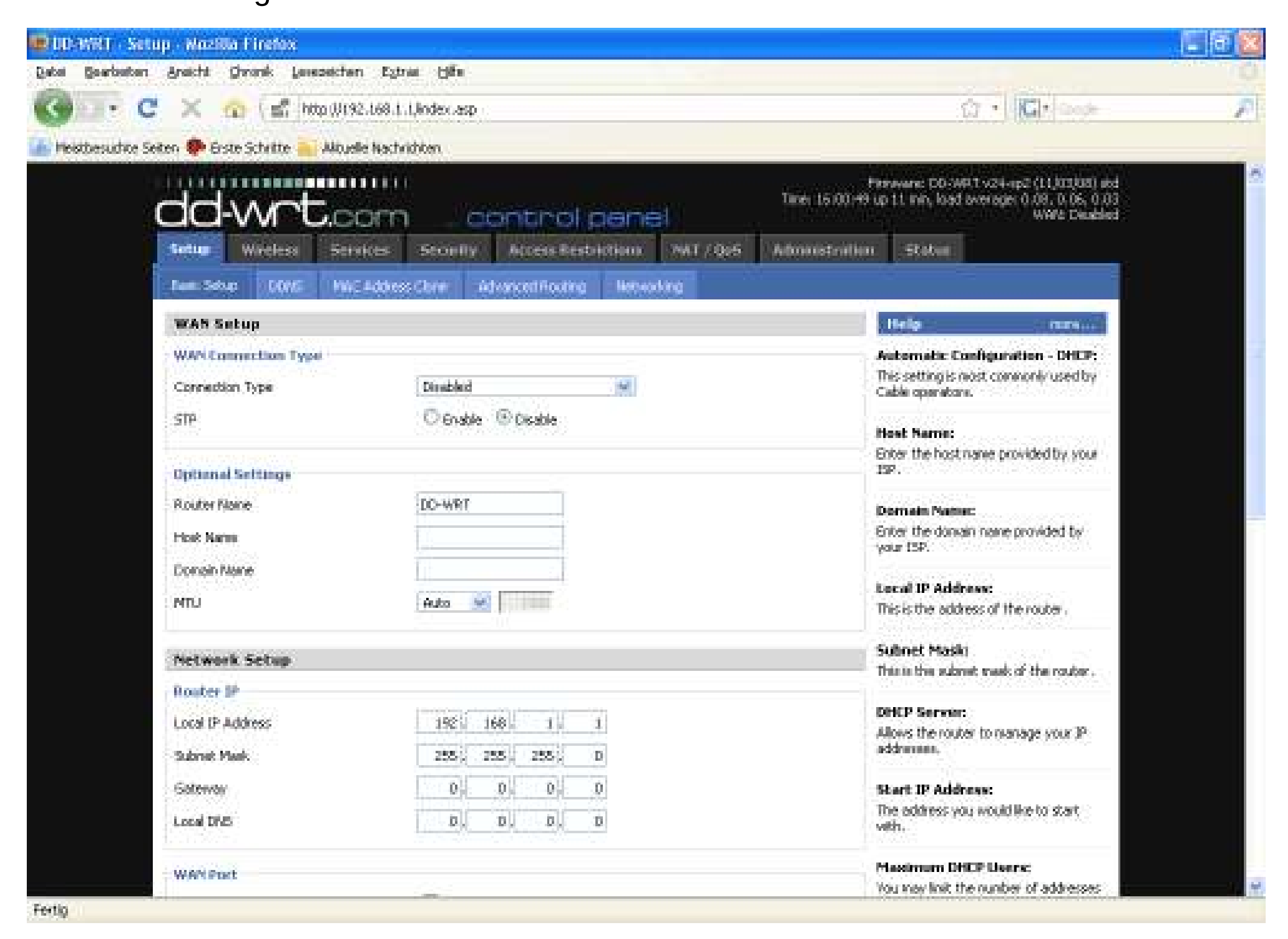


2.3. Struktur des Webinterface



2.3.1. Setup

2.3.1.1. Grundeinrichtung



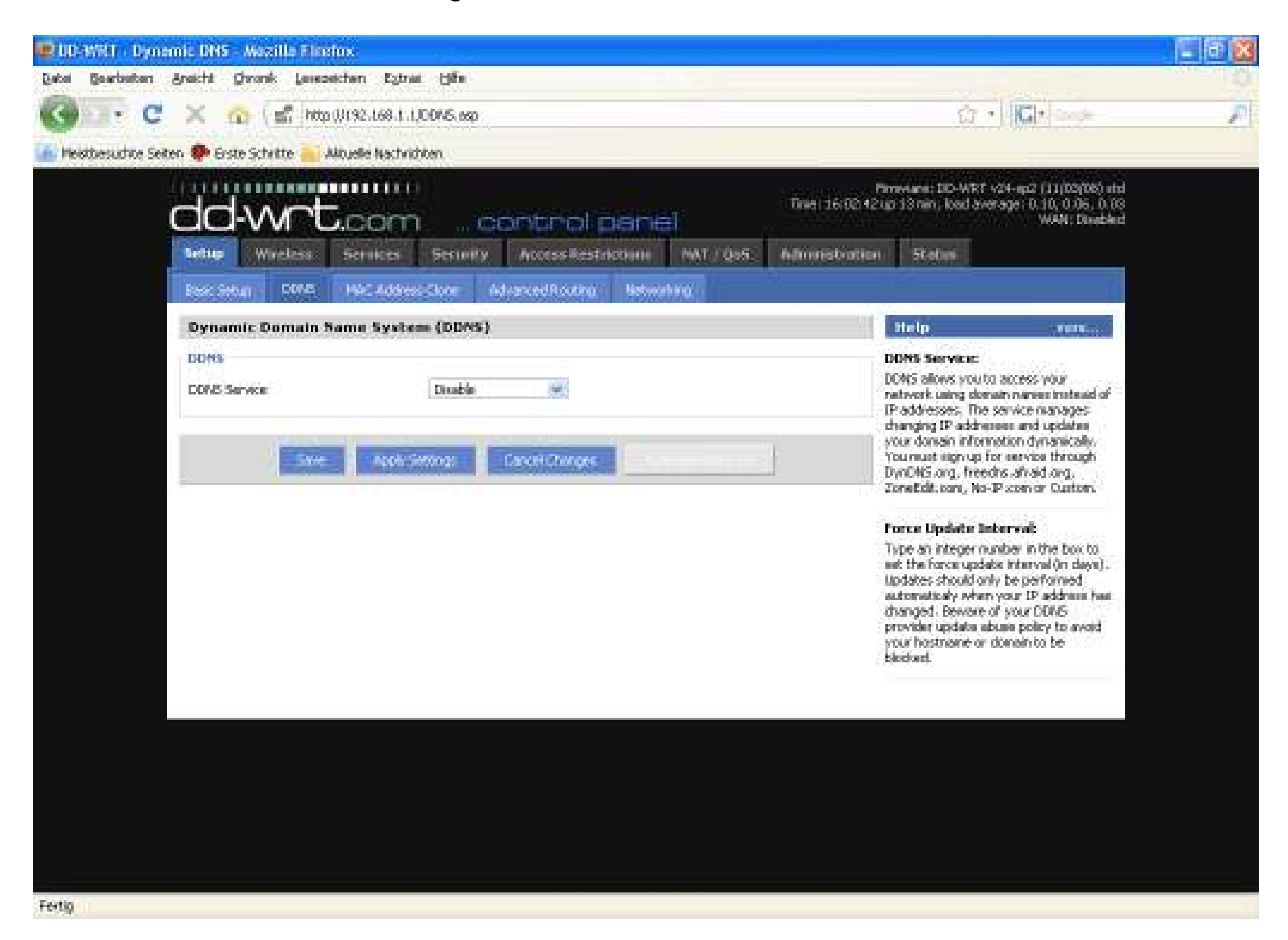
Internet Setup
Hier sind die wesentlichen Einstellungen für die Internet-Anbindung, sprich den WAN-Port, zu finden. Neben dem voreingestelllten Modus DHCP stehen auch PPPoE, PPTP, L2TP, statische IP swie das exotischere HeartBeat Signal zur Verfügung. Im Falle, dass der ISP keine Passwörter vergibt (z.B. Alice) muss z.B. „0000“ als Passwort angegeben werden. Ebenfalls ist zu beachten, dass bei manchen Anbietern der Service-Name richtig geschrieben sein muss, sonst kann die Anmeldung fehlschlagen. In einem solchen Fall empfiehlt es sich, den Service-Namen leer zu lassen.

WAN Connection Type	Beschreibung
Disabled	Das WAN-Interface ist deaktiviert
Static IP	Verwendung einer festen IP-Adresse – In diesem Fall müssen IP-Adresse, Netzmaske, Gateway und Server eingetragen werden
Automatic Configuration - DHCP	Die IP-Adresse wird von einem DHCP-Server bezogen
PPPoE	Konfiguration als PPPoE-Client, bei VDSL muss die Checkbox „VDSL-Tagging“ gesetzt werden
PPTP	Verbindungsaufbau per PPTP
L2TP	Verbindungsaufbau per L2TP
HeartBeat Signal	Nutzung im Zusammenhang mit einem HeartBeat-Signal, nur bei bestimmten Providern erforderlich (in Europa unüblich)

Network Setup
Das Network Setup umfasst die grundlegenden Einstellungen für das lokale Netzwerk. Die hier vorgenommenen Einstellungen beziehen sich auf die komplette Bridge, d.h. auch auf die WLAN-Interfaces, sofern diese nicht aus der Bridge entfernt wurden.

2.3.1.2. Dynamic DNS (DynDNS oder DDNS)

Beim Dynamic DNS handelt es sich um einen Dienst, bei dem auch Geräte mit einer dynamisch zugewiesenen offiziellen IP-Adresse ein gültiger DNS-Eintrag zugewiesen werden kann. Um einen solchen Dienst nutzen zu können muss auf dem Router ein DynDNS Client aktiv sein, der bei Änderungen an der IP-Adresse den externen DynDNS-Dienst über diese Änderung informiert und so die DNS-Einträge zeitnah aktualisiert.



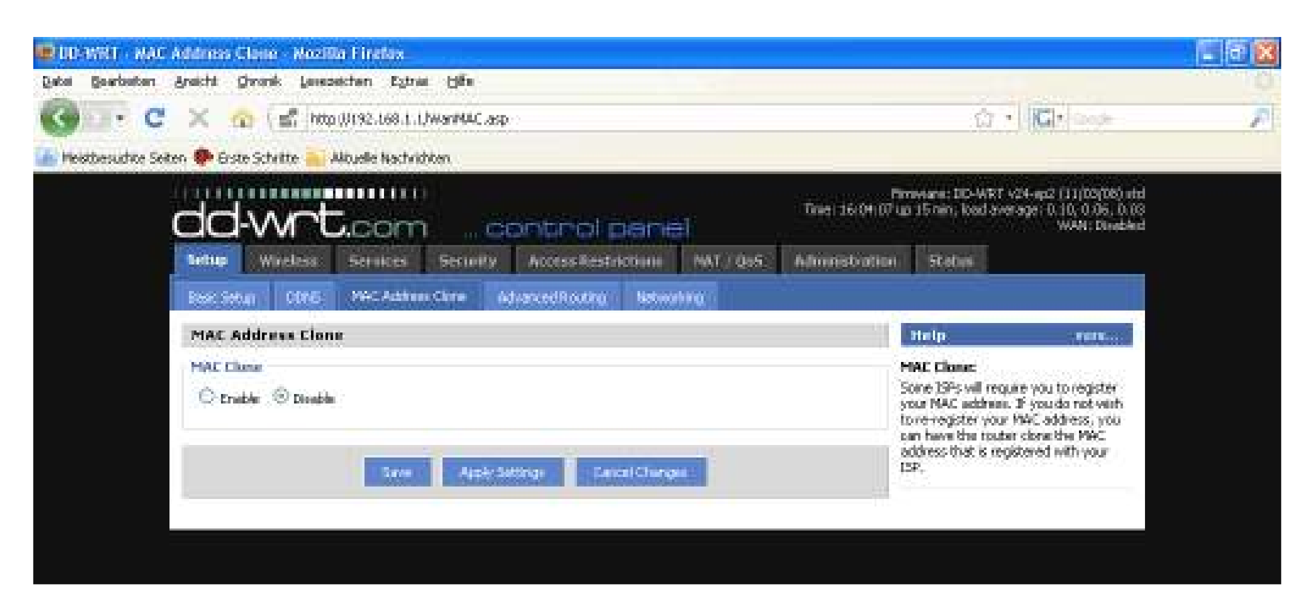
Die Router-Firmware bietet Unterstützung für die gängigen DynDNS-Serviceanbieter sowie eine Option zur Definition eigener Einstellungen.

DynDNS Service	Beschreibung
Disabled	Voreinstellung, kein DynDNS
DynDNS.org	
freedns.afraid.org	
ZoneEdit.com	
No-IP.com	
3322.org	
easyDNS.com	
TZO.com	

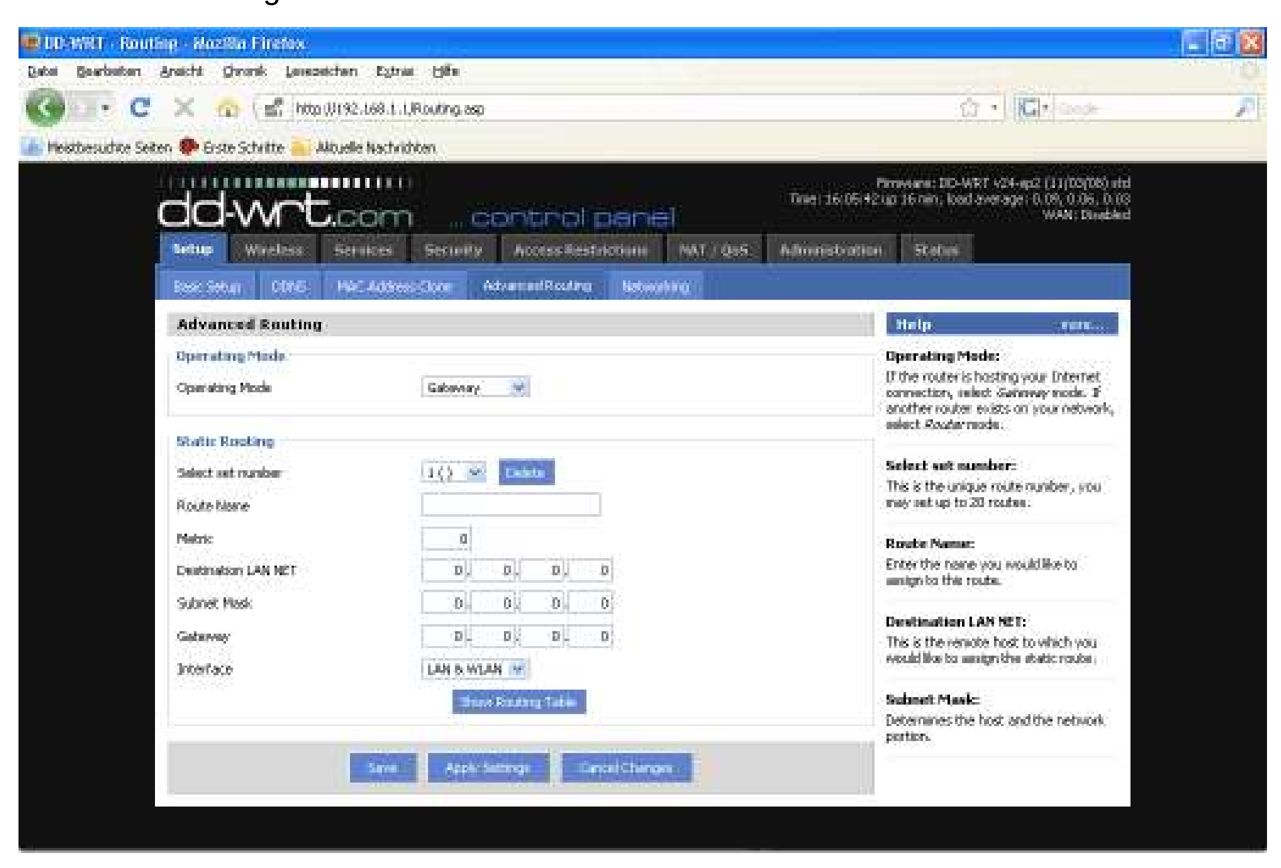
DynSIP.org	
Custom	Erlaubt eigene Einstellungen zur Unterstützung weiterer DynDNS-Dienste

2.3.1.3. MAC-Adresse Clone

MAC-Adress cloning erlaubt es, dem LAN- oder einem WLAN-Interface virtuell eine andere als die in der Hardware kodierte MAC-Adresse zu verwenden.



2.3.1.4. Advanced Routing

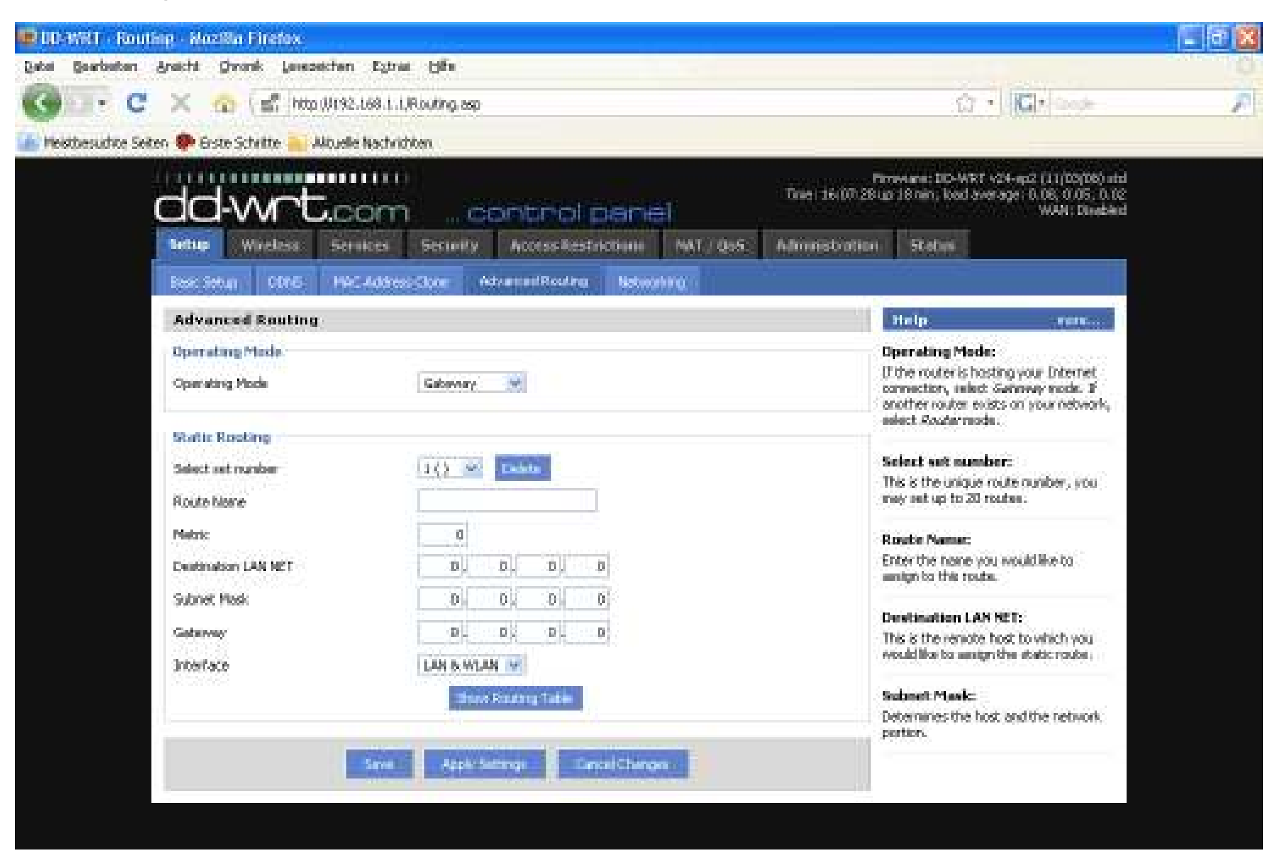


Operating Mode
Die Einstellungen unter „Advanced Routing" erlauben die Verwendung weiterer Routingprotokolle, der Standard-Betriebsmodus ist „Gateway".

Modus	Beschreibung
Gateway	Voreinstellung, normaler Betrieb als Gateway
BGP	Betrieb als Router mit BGP-Routing
Rip2 Router	Betrieb als Router mit Rip2-Routing
OSPF Router	Betrieb als Router mit OSPF-Routing
OLSR Router	Betrieb als Router mit OLSR-Routing
Router	Betrieb als „normaler" Router

Static Routing
Über die Einstellungen unter „Static Routing" können statische Routen hinzugefügt werden. Die Eingabeparameter entsprechenden denen des Linux-Kommandos „route".

2.3.1.5. Networking



Im Bereich „Networking" können verschiedene weitere Einstellungen vorgenommen werden.

VLAN Tagging
Diese Option wird benötigt, wenn VLANs eingerichtet werden sollen.

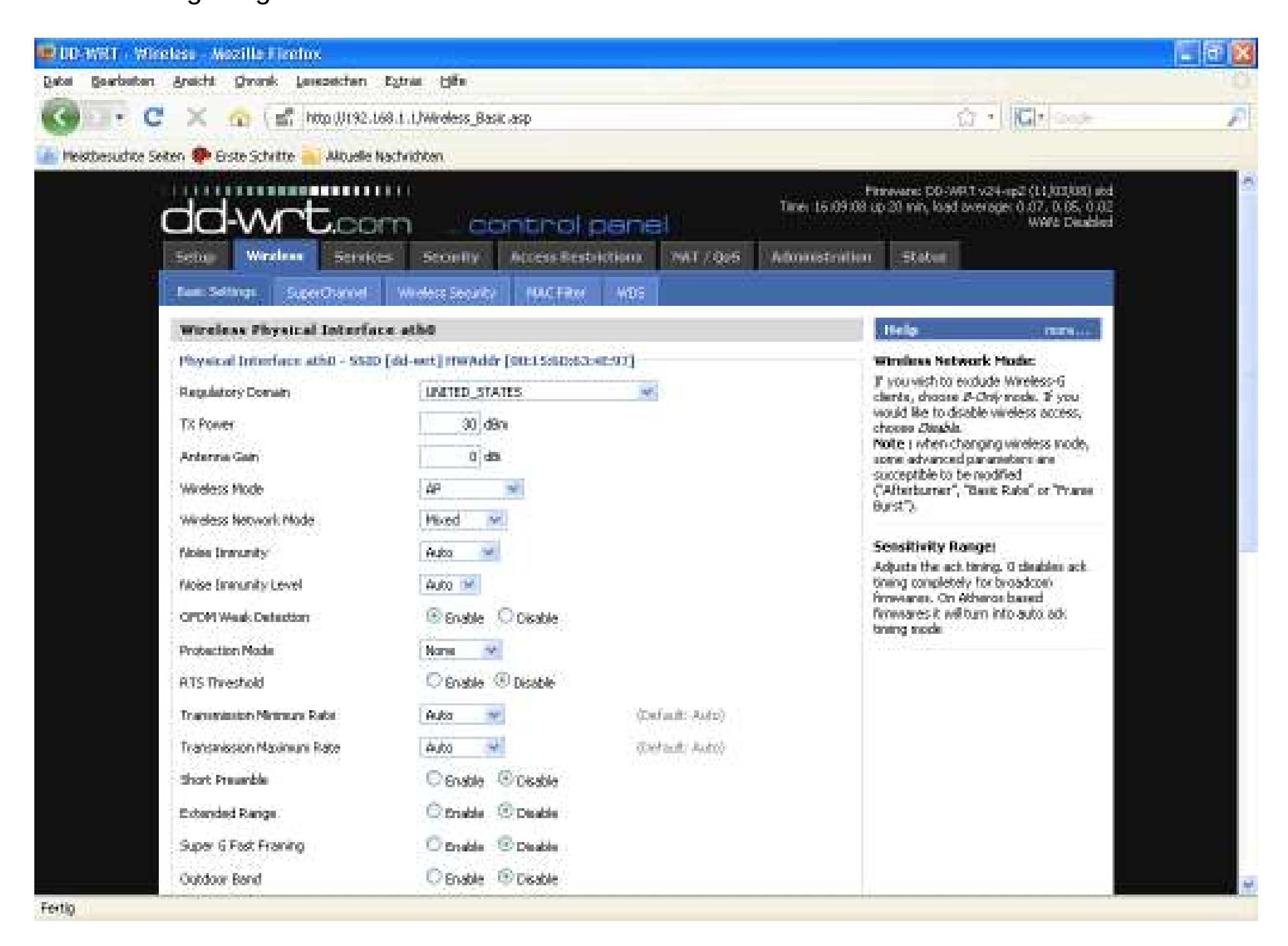
Bridging
Per default ist eine Bridge (br0) aktiv. Über diesen Punkt können weitere Bridges definiert und die Inferfaces den verschiedenen Bridges zugeordnet werden.

DHCPD
Neben dem Standard-DHCP-Server ist es möglich weitere virtuelle DHCP-Server einzurichten.

2.3.2. Wireless

2.3.2.1. Grundeinstellungen

Für jedes WLAN Interface existiert eine Rubrik in den Grundeinstellungen. Die WLAN Interfaces sind mit ath0 – ath4 (bei einem System mit 4 mini-PCI-Steckplätzen) benannt. Die Reihenfolge wird intern an den mini-PCI-Steckplätzen festgemacht, für die Zuordnung zu den Antennen vergleichen Sie bitte die MAC-Adressen auf den Gehäusen mit den Adressen, die für das Interface angezeigt werden.



Regulatory Domain
Über diese Auswahl werden die Rahmenbedingungen für das Einsatzland definiert, d.h. die nutzbaren Kanäle im 2.4 GHz und 5 GHz Band sowie die zulässigen Sendeleistungen.

TX Power & Antenna Gain
Diese beiden Werte stehen in einem engen Zusammenhang. Damit die regulatorischen Vorgaben eingehalten werden, kann an dieser Stelle der Antennengewinn in dbm eingegeben werden. Das System regelt dann die Sendeleistung so, dass bei der Abstrahlung an der Antenne die vorgegebenen Grenzwerte der Sendeleistung eingehalten werden.

Wireless Mode
Über diesen Parameter wird der Betriebsmodus für das WLAN Interface definiert. Die folgenden Modi stehen zur Auswahl:

Modus	Beschreibung
AP	Voreinstellung, Betrieb als WLAN Access Point
Client	Betrieb als WLAN-Client
Client-Bridge	Betrieb als Client-Bridge, d.h. mit Hilfe eines weiteren virtuellen AP’s kann auf dem gleichen Interface über eine virtuelles WLAN-Interface ein AP bereitgestellt werden.
AdHoc	Betrieb AdHoc-Gerät
WDS AP	Betrieb als WDS AP, die Besonderheit ist, dass mit WDS-AP / WDS-Station auf der Station eine transparente Bridge erzeugt. Der Modus WDS-AP / WDS-Station wird auch für Punkt-zu-Punkt Verbidnungen empfohlen.
WDS Station	Betrieb als WDS Station – Gegenstück zum WDS AP

Wireless Network Mode
Hier wird der Grundbetriebsmodus bezüglich des verwendeten IEEE802.11 Standards definiert.

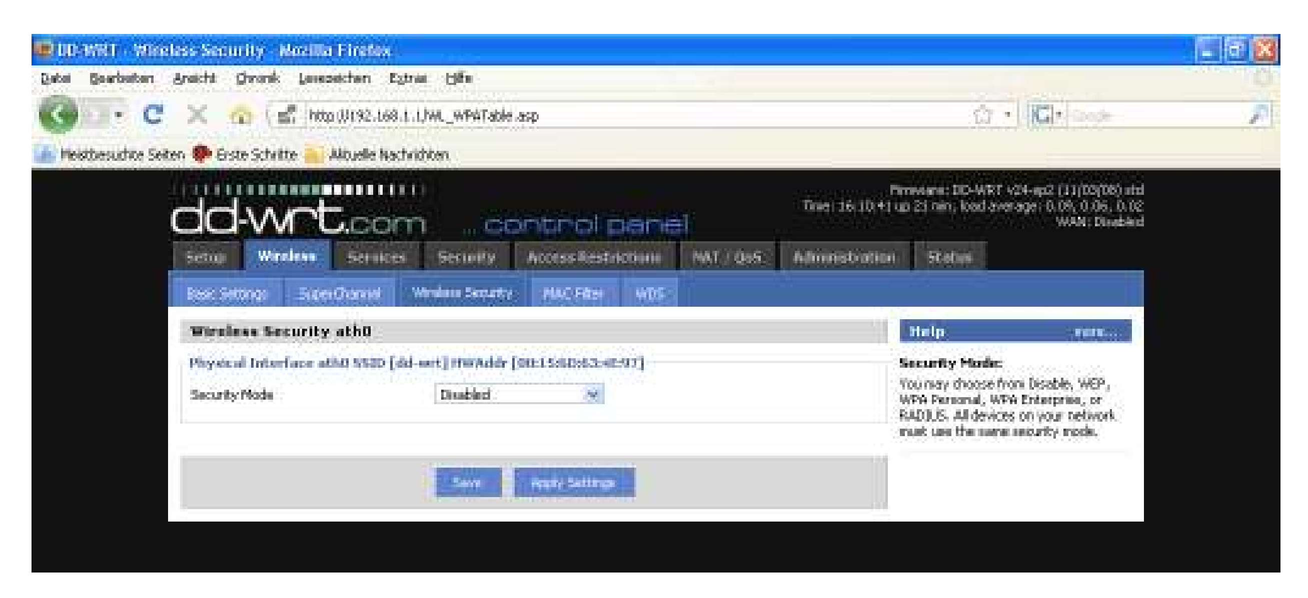
Modus	Beschreibung
Disabled	Das Interface ist inaktiv
A-Only	Betrieb im 5 GHz Band
B-Only	Betrieb im 2,4 GHz Band, 802.11b – Verbindungen zu Geräten mit 802.11g sind nicht möglich
G-Only	Betrieb im 2,4 GHz Band, 802.11g – Verbindungen zu Geräten mit 802.11b sind nicht möglich
BG-Mixed	Gemischter Betrieb zwischen 802.11b und 802.11g

Scanlist
Insbesondere im 5Ghz Outdoor Band ist der Frequenzbereich sehr groß. Wenn der Router in einem der Client Modi betrieben wird, dann scannt er nach dem Einschalten alle verfügbaren Frequenzen nach einem zugehörigen AP. Das kann mitunter mehrere Minuten dauern. Um diesen Vorgang zu beschleunigen können in der Scanlist Frequenzen als 4-stellige Ganzzahl (z.B. 5660 für 5,6 GHz) kommagetrennt eingetragen werden. Dadurch wird nur auf den angegebenen Frequenzen nach einem Access Point gesucht.

Sensivity Range (ACK Timing)
Dieser Wert bestimmt das ACK-Timing und sollte mindestens so groß sein, wie die Distanz zum Access Point. Wenn der Wert auf 0 gesetzt wird, wird der Wert automatisch bestimmt.

2.3.2.2. Wireless Security

WLAN-Verbindungen unterliegen aufgrund der drahtlosen Übertragung erhöhten Anforderungen an die Absicherung der Datenübertragungen.



Security Mode

Modus	Beschreibung
Disabled	Keine Verschlüsselung – für den Regelbetrieb nicht empfehlenswert
WPA Personal	WPA Verschlüsselung mit einer Passphrase (Text-Kennwort)
WPA Enterprise	WPA Verschlüsselung mit Radius Client Authentifizierung nach 802.1x
WPA2 Personal	WPA2 Verschlüsselung mit einer Passphrase (Text-Kennwort)
WPA2 Enterprise	WPA2 Verschlüsselung mit Radius Client Authentifizierung nach 802.1x
WPA2 Personal Mixed	WPA & WPA2 Verschlüsselung im Mischbetrieb mit einer Passphrase (Text-Kennwort)
WPA2 Enterprise Mixed	WPA & WPA2 Verschlüsselung im Mischbetrieb mit Radius Client Authentifizierung nach 802.1x
RADIUS	
WEP	WEP 64 Bit oder 128 Bit Verschlüsselung – aufgrund der konzeptionellen Sicherheitsproblematik wir vom Einsatz von WEP abgeraten!

Bei der (nicht empfohlenen) Verwendung von WEP als Verschlüsselungsverfahren kann zwischen 64 und 128 Bit langen Schlüsseln gewählt werden. Die Eingabe kann auch über eine Passphrase erfolgen, aus der die Hex-Schlüssel erzeugt werden. Theoretisch bieten 128 Bit lange Schlüssel ein höheres Maß an Sicherheit, aufgrund der bekannten Angriffsmethoden spielt das aber in der Praxis keine Rolle mehr.

Schlüssellänge	Beschreibung
64 Bit (10 Hexadezimalzeichen)	Standard
128 Bit (26 Hexadezimalzeichen)	

Wenn als Verschlüsselungstyp „WPA“oder „WPA2“gewählt werden, stehen verschiedene Verschlüsselungsalgorithmen zur Verfügung. Leider gibt es keine generelle Empfehlung, welche Algorithmus in allen Fällen richtig ist. Wenn Sie sich unsicher sind, verwenden Sie am besten TKIP.

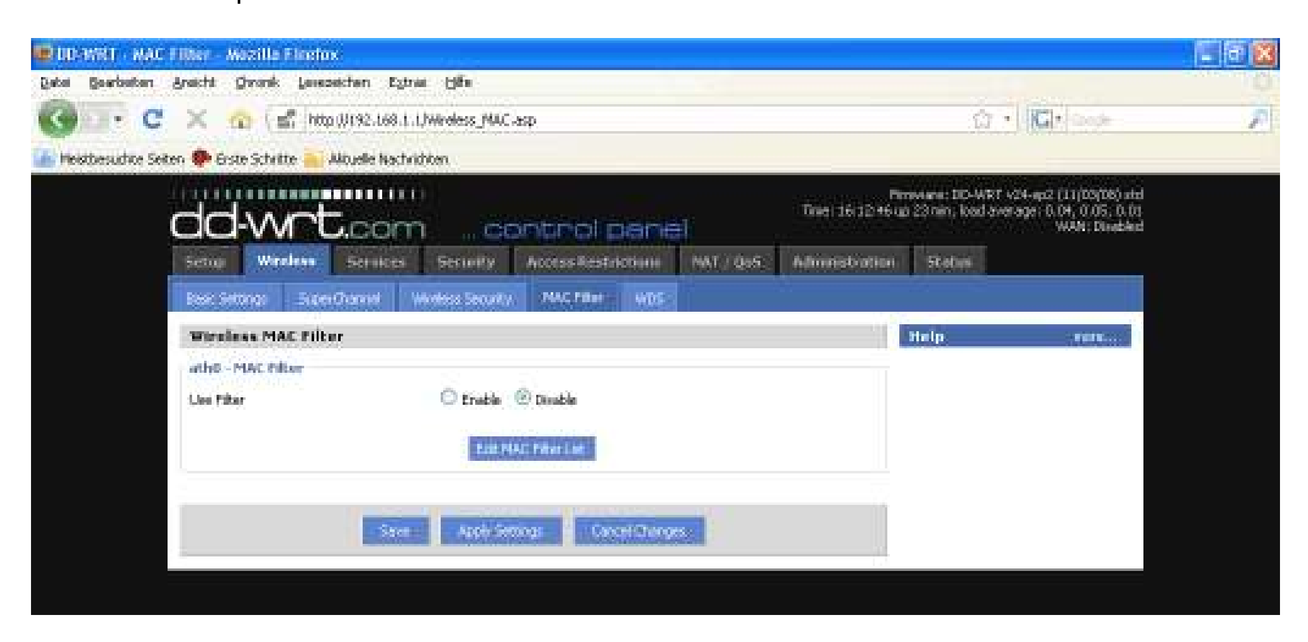
Algorithmus	Beschreibung
TKIP	TKIP Verschlüsselung, wir von den meisten Client-Geräten unterstützt
AES	AES Verschlüsselung bietet ein höheres Maß an Sicherheit und ist of ressourcenschonender, wir aber von manchen Client-Geräten nicht uterstützt.
TKIP + AES	Mischbetrieb zwischen TKIP & AES – bietet Höchstmaß an Kompatibilität, kann aber in manchen Umgebungen zu Problemen führen

Bei der Nutzung des Sicherheitsmodus „RADIUS“ das entsprechende Format für die eingegebenen MAC-Adressen definiert werden.

RADIUS MAC Formatoptionen	Beschreibung
aabbcc-ddeeff	Standard
aabbccddeeff	
aa:bb:cc:dd:ee:ff	
aa-bb-cc-dd-ee-ff	

2.3.2.3. MAC Filter

Über die MAC Filter-Funktionalität können MAC-Adressen von Geräten definiert werden, die sich am Accesspoint anmelden dürfen.



2.3.2.4. WDS

Wireless Distribution System (WDS) ist ein spezieller Accesspoint-Modus der es erlaubt, mehrere Accesspoints per WLAN zu einem gemeinsamen Netz zusammenzuschalten und kann z.B. für die Erweiterung der Netzabdeckung verwendet werden.

Als WDS-Nodes werden die MAC-Adressen der nächstgelegenen Accesspoints, mit denen sich der aktuelle verbinden soll, eingetragen. Man sollte dabei „doppelte“ Strecken, d.h. A <-> B + A <-> B <-> C, vermeiden. Die folgenden Modi stehen für die Koppelung der WDS Knoten zur Verfügung:

WDS Client Mode	Beschreibung
disabled	Standard
Point-to-Point	Üblicherweise wird dieser Modus verwendet
LAN	

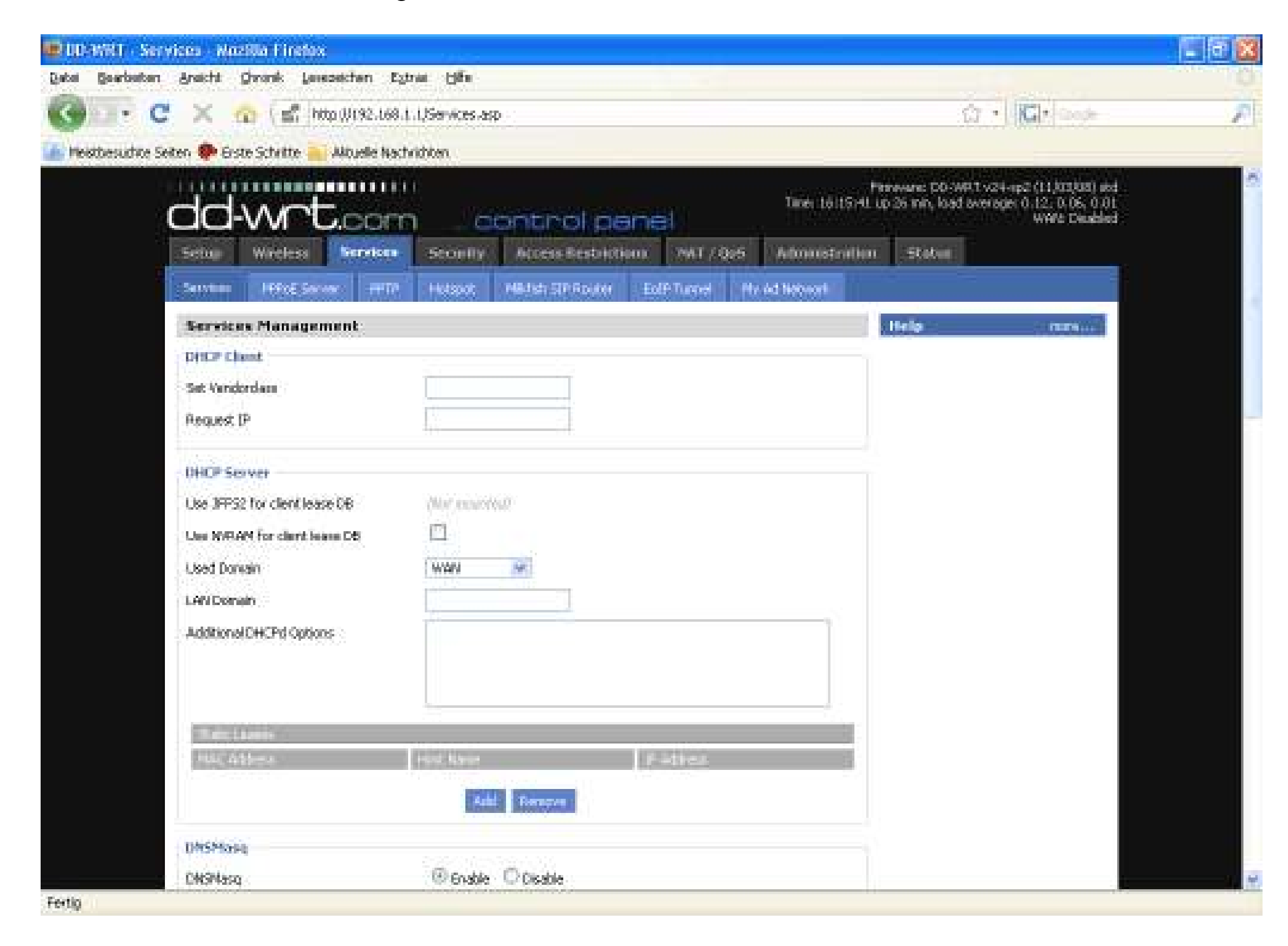
Wenn WDS aktiviert ist kann außerdem der NAT-Modus eingestellt werden:

WDS NAT Mode	Beschreibung
WLAN -> WDS	Standard
WDS -> WLAN	

2.3.3. Services

2.3.3.1. Services

Im Services-Tab können die grundlegenden Dienste-Einstellungen gesetzt werden. Insbesondere Telnet und SSH sind hierüber konfigurierbar. Die Fernkonfiguration wird aber im Bereich „Administration“ eingerichtet.

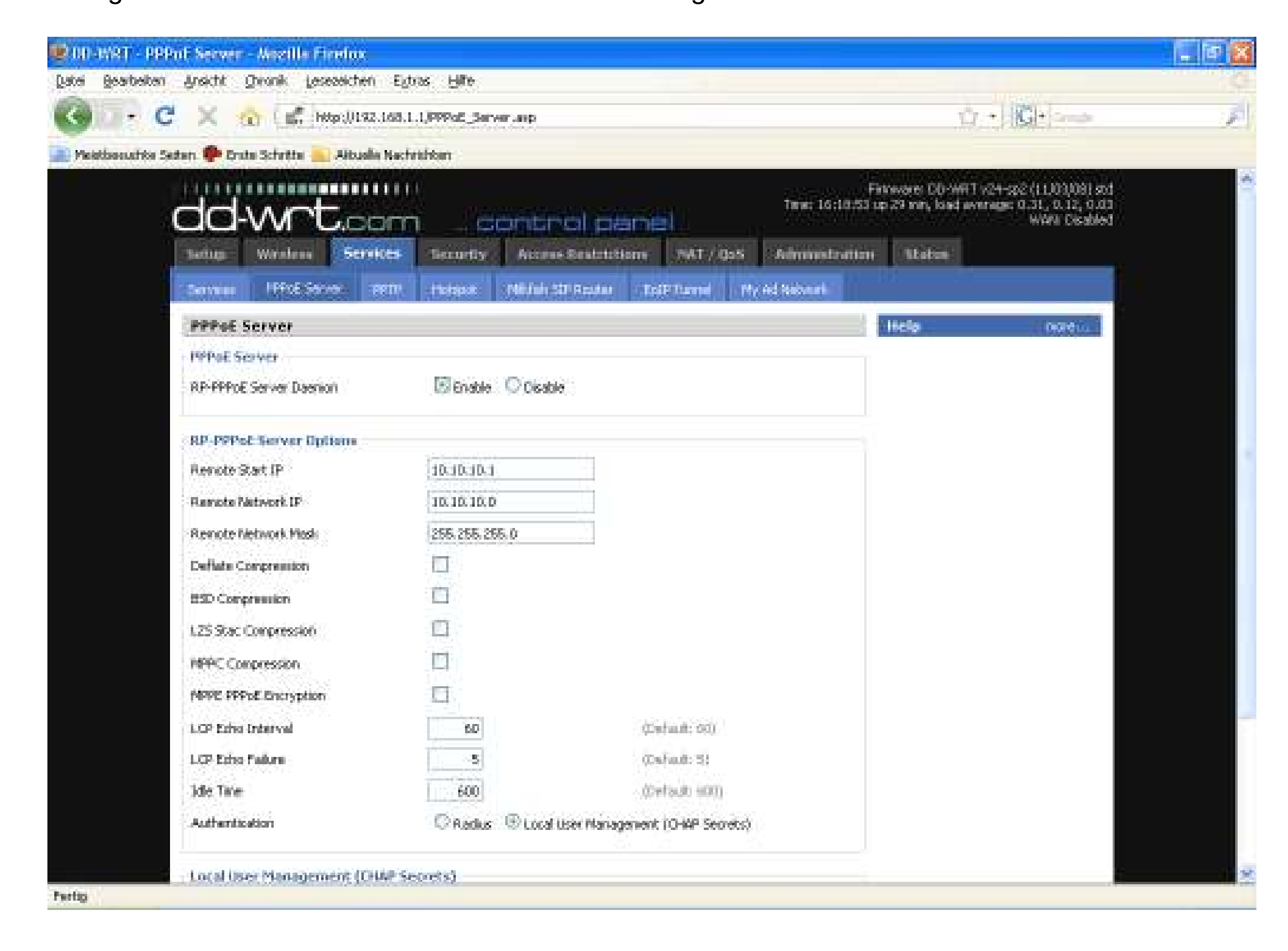


Verfügbare DHCP Server Domains	Beschreibung
WAN	Standard
LAN / WLAN	

Rflow / MACupd Interface Options	Beschreibung
LAN & WLAN	Standard
LAN	
WLAN	

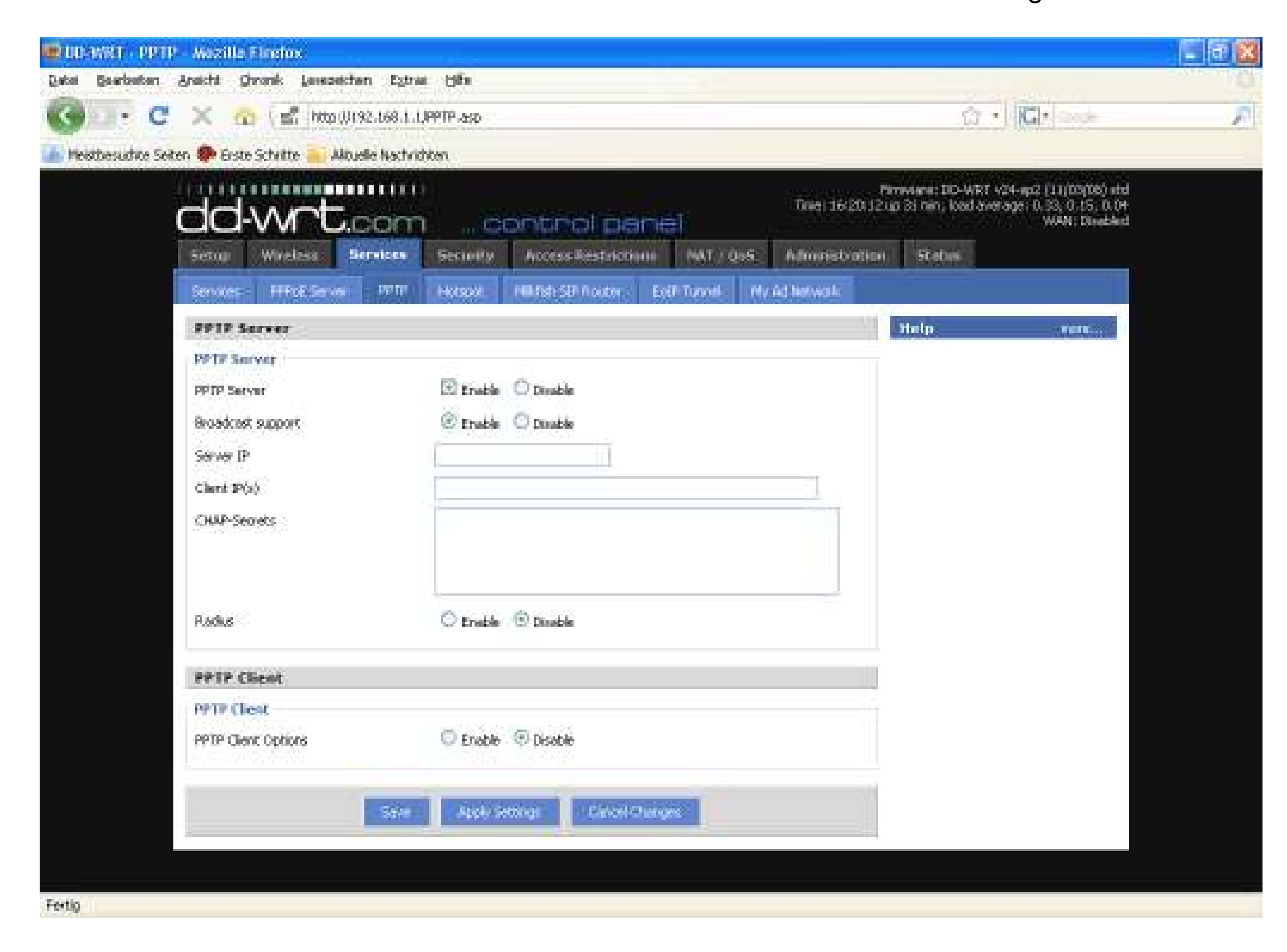
2.3.3.2. PPPoE Server

Für manche Anwendungen ist der Betrieb eines PPPoE-Servers sinnvoll, welcher hier konfiguriert werden kann. In der Standardeinstellung ist der PPPoE-Server deaktiviert.



2.3.3.3. PPTP

Der Router kann bei Bedarf auch als PPTP-Server oder als PPTP-Client konfiguriert werden.



Bei der Angabe des IP-Bereichs sollten Überschneidungen mit dem DHCP-Bereich (sofern DHCP aktiviert wurde) vermieden werden. Der IP-Bereich der Clients wird mit folgender Syntax eingegeben:

xxx.xxx.xxx.<start-ip>-<end-ip>

also z.B.

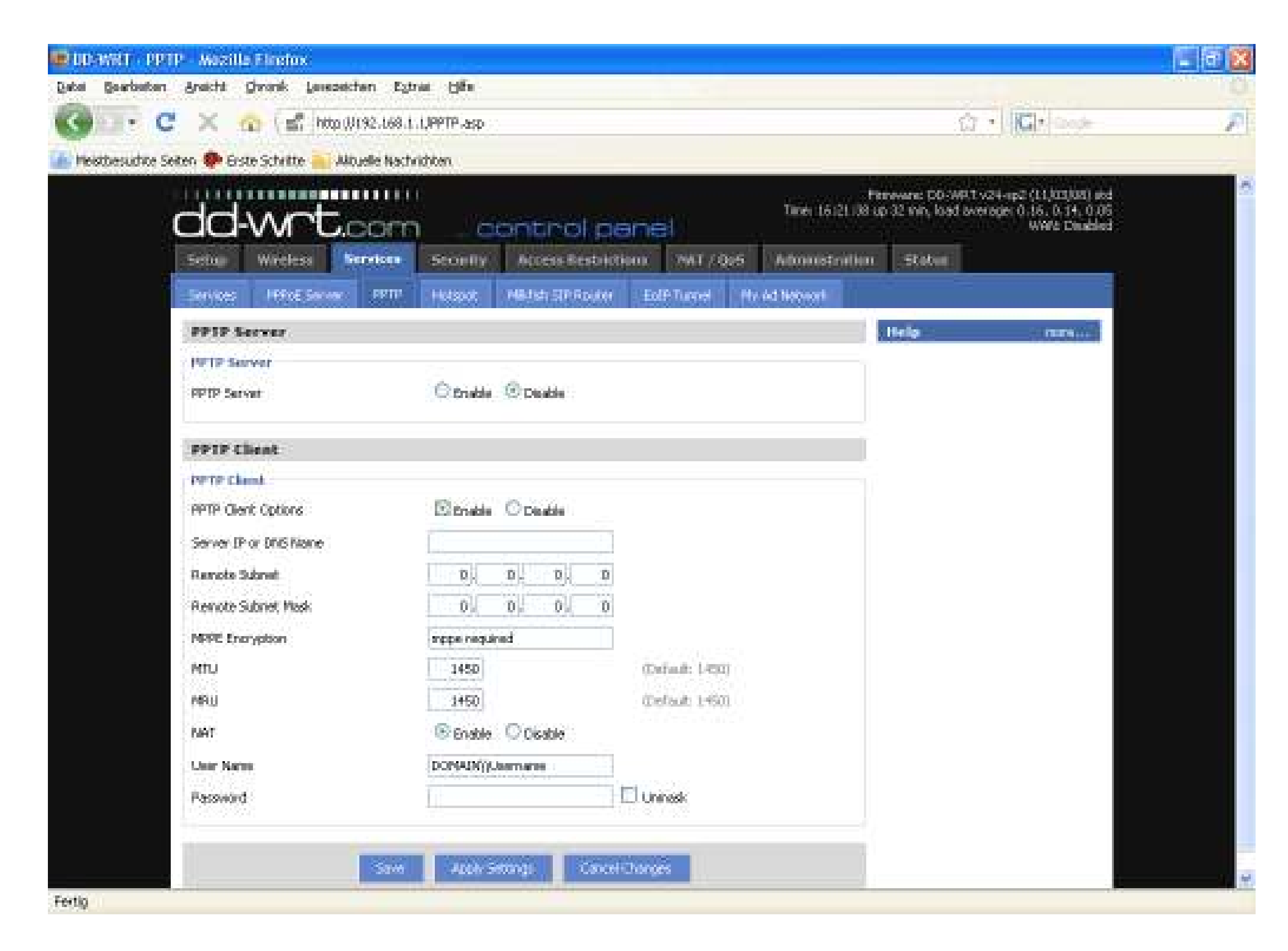
192.168.1.20-30

Die Anmeldedaten der Clients werden wie folgt zeilenweise in das entsprechende Feld eingegeben:

<username> * <password> *

also z.B.

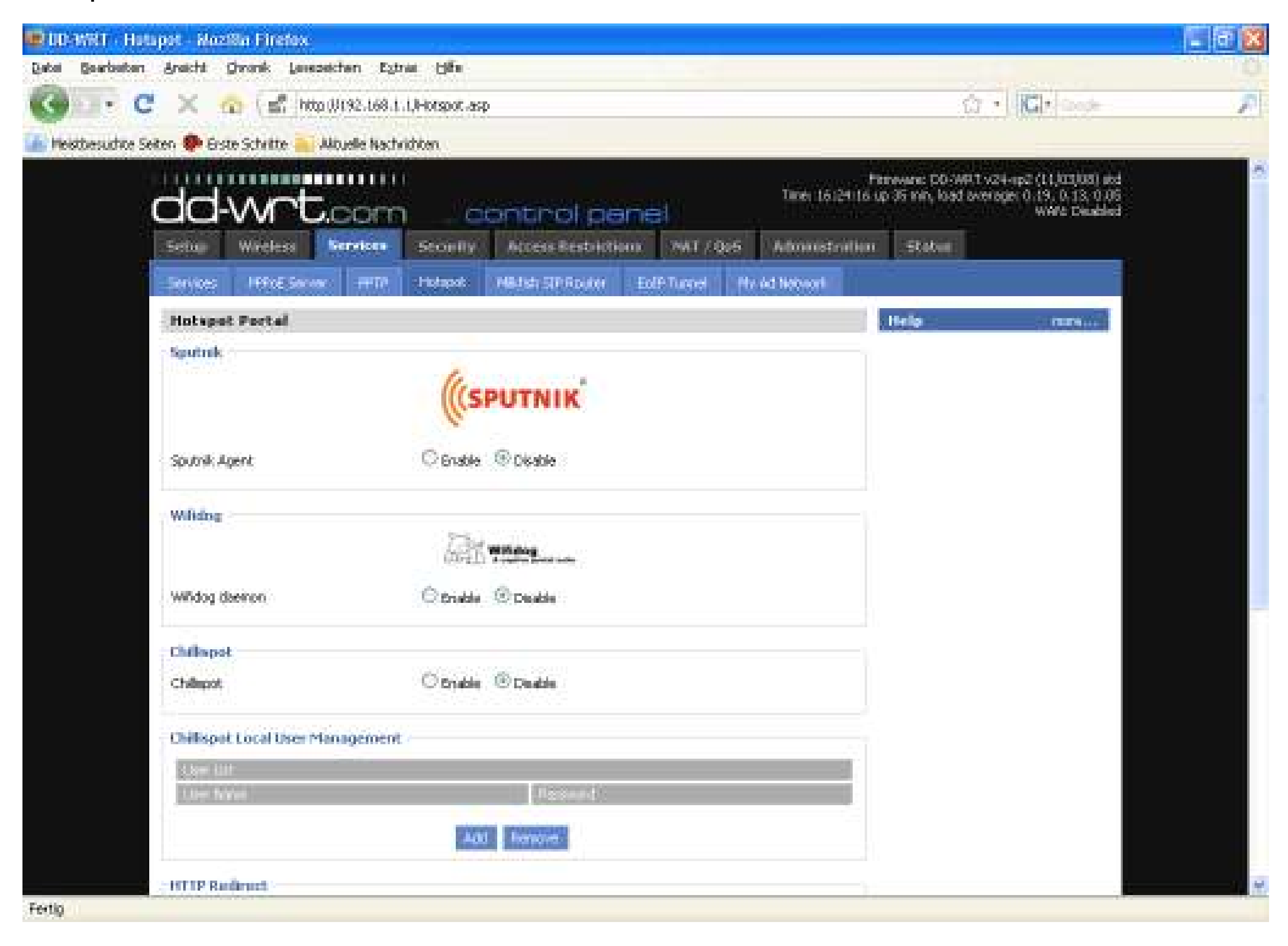
testbenutzer * test *



Hier sind die folgenden Einstellungen für die Verschlüsselung zu beachten:

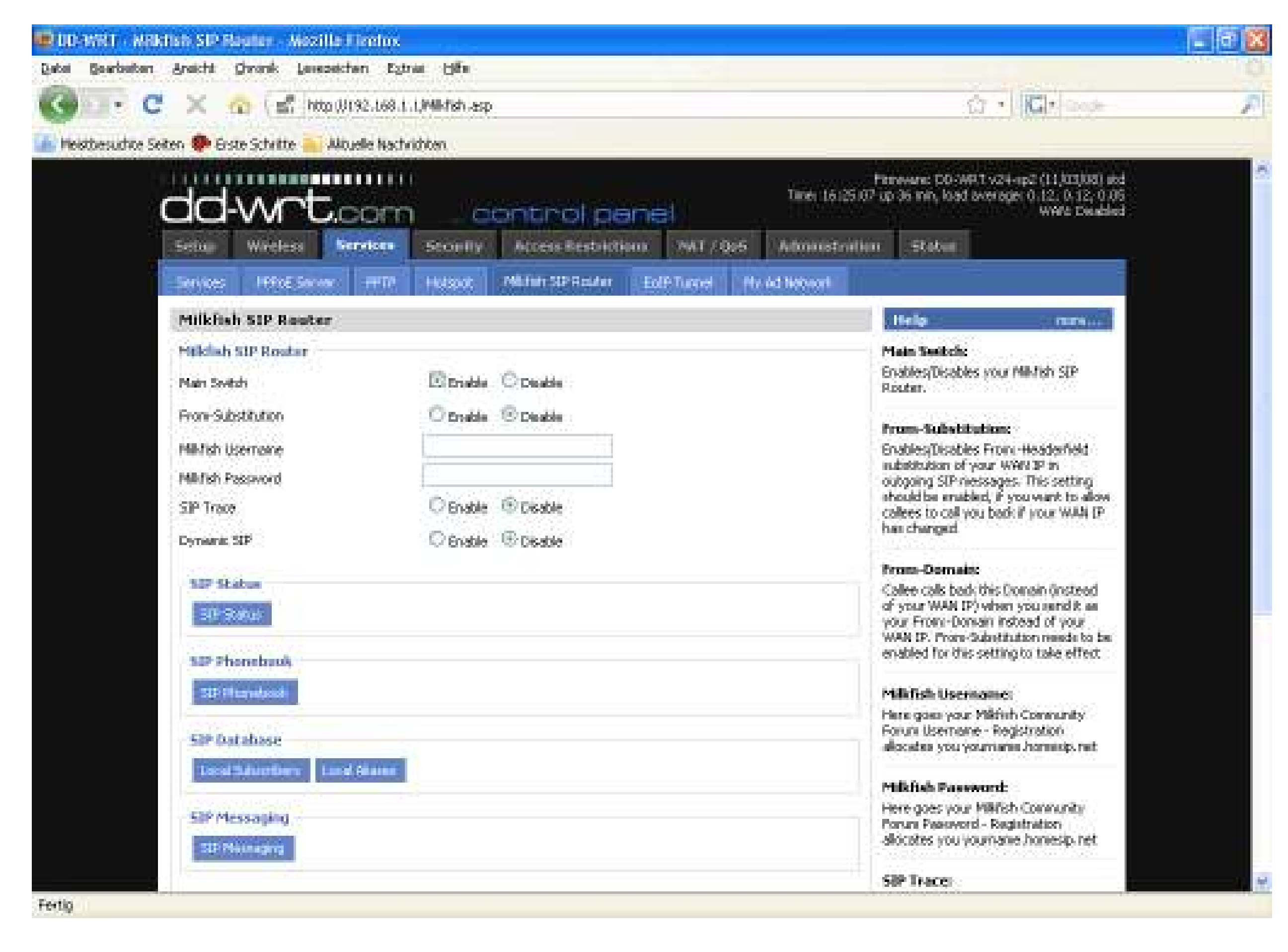
Gegenstelle	Einstellungen
DD-WRT Router	mppe required (Standard)
Windows PPTP Server	mppe required,no40,no56,stateless *oder* mppe required,no40,no56,stateful

2.3.3.4. Hotspot



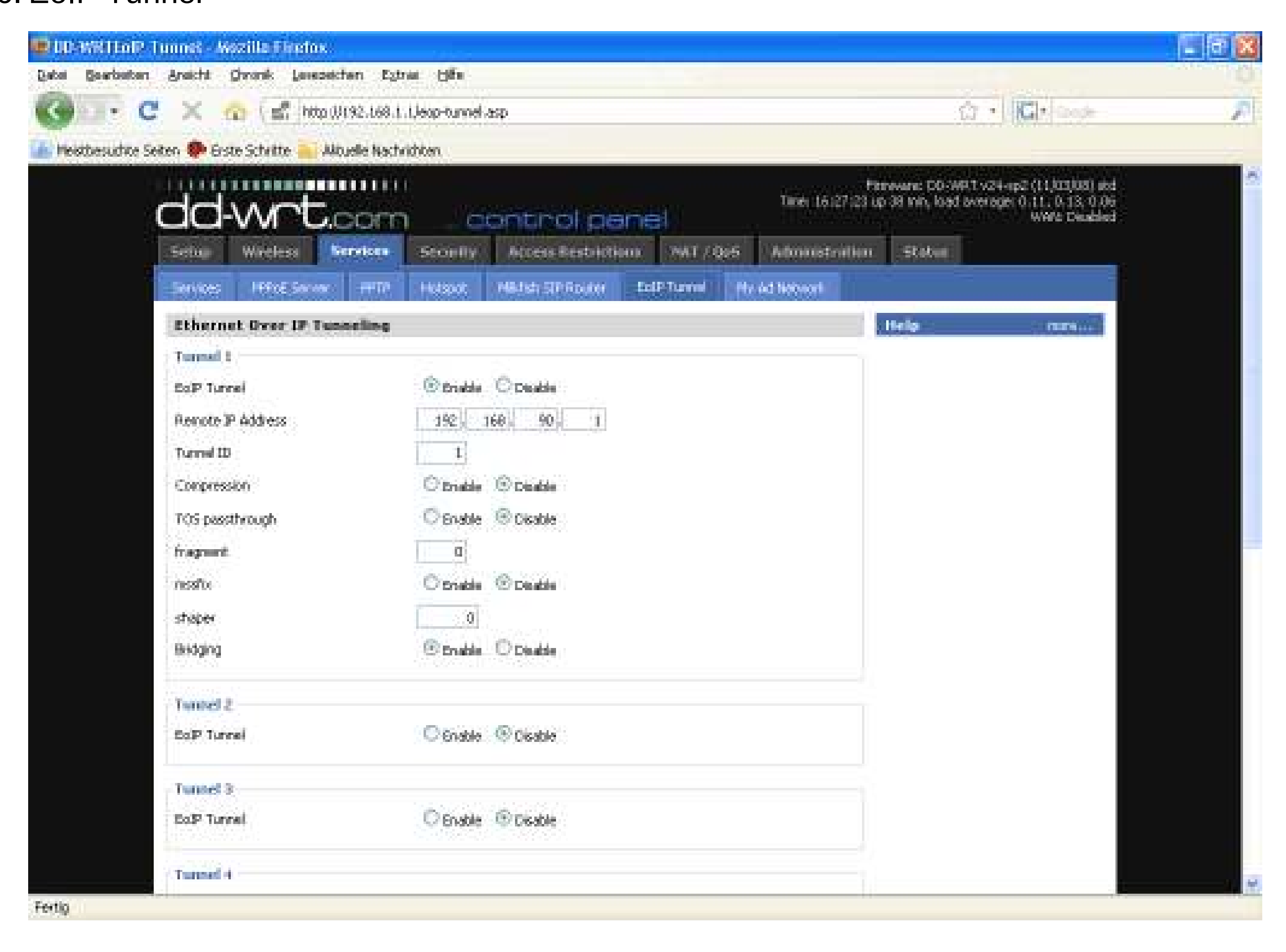
Die verschiedenen Hotspot-Dienste benötigen in den meisten Fällen einen entsprechenden Server. Zu beachten ist, dass es sich bei Sputnik um ein kommerzielles Hotspot-System handelt und die Nutzung eine entsprechende Vereinbarung mit Sputnik erfordert.

2.3.3.5. Milksfish SIP Router



Milkfish ist ein SIP-Router und erfordert einen Milkfish Benutzeraccount (www.milkfish.org).

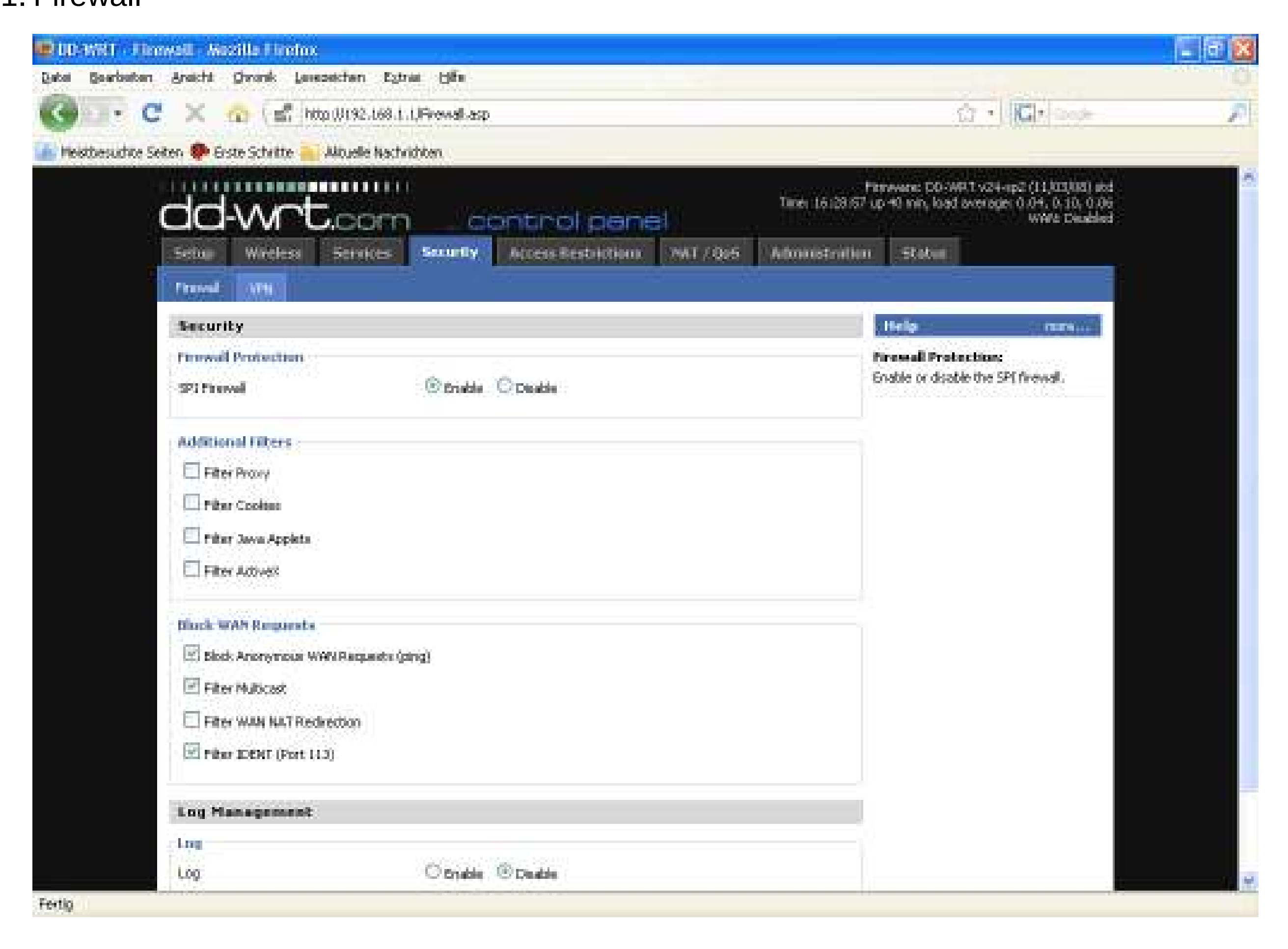
2.3.3.6. EoIP Tunnel



Mit Hilfe der EoIP Tunnel-Funktion können über das IP-Protokoll Ethernet-Tunnel generiert werden. Das Interface bietet die Möglichkeit, bis zu zehn EoIP-Tunnel einzurichten.

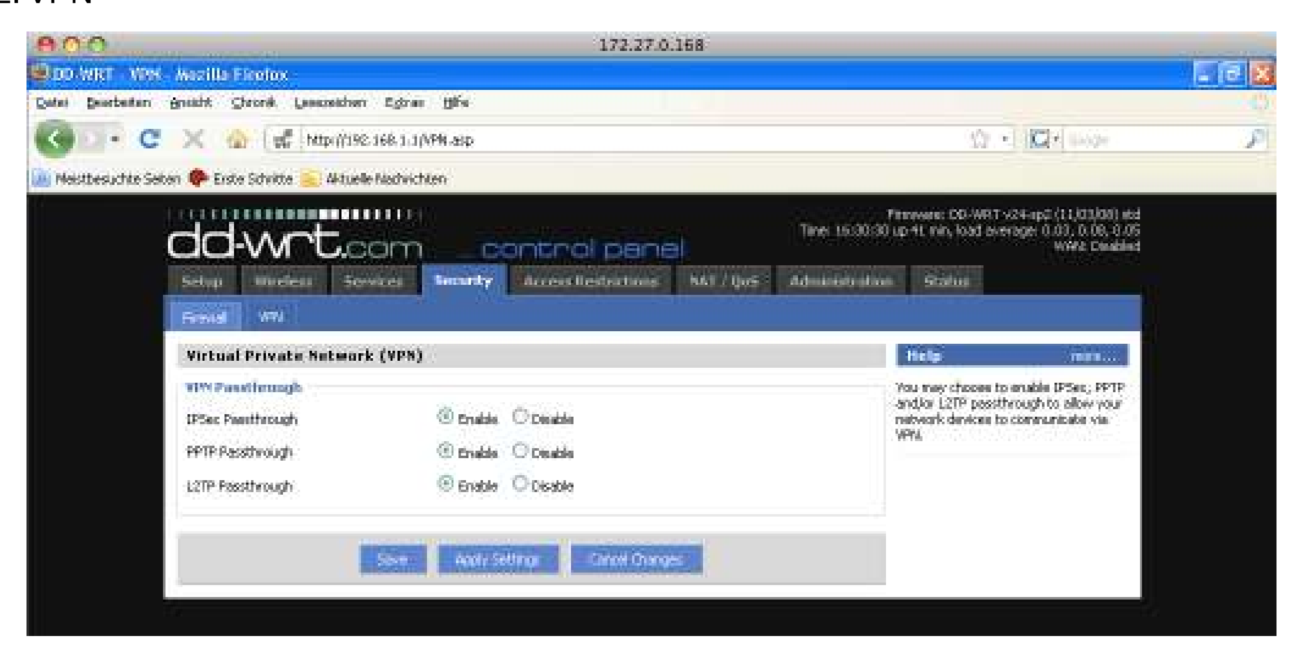
2.3.4. Security

2.3.4.1. Firewall



Neben der Möglichkeit, die Firewall zu aktivieren bzw. zu deaktivieren können hier die Einstellungen für zusätzliche Filter, zum Blocken bestimmter Anfragen an das WAN-Interface und das Logmanagement vorgenommen werden.

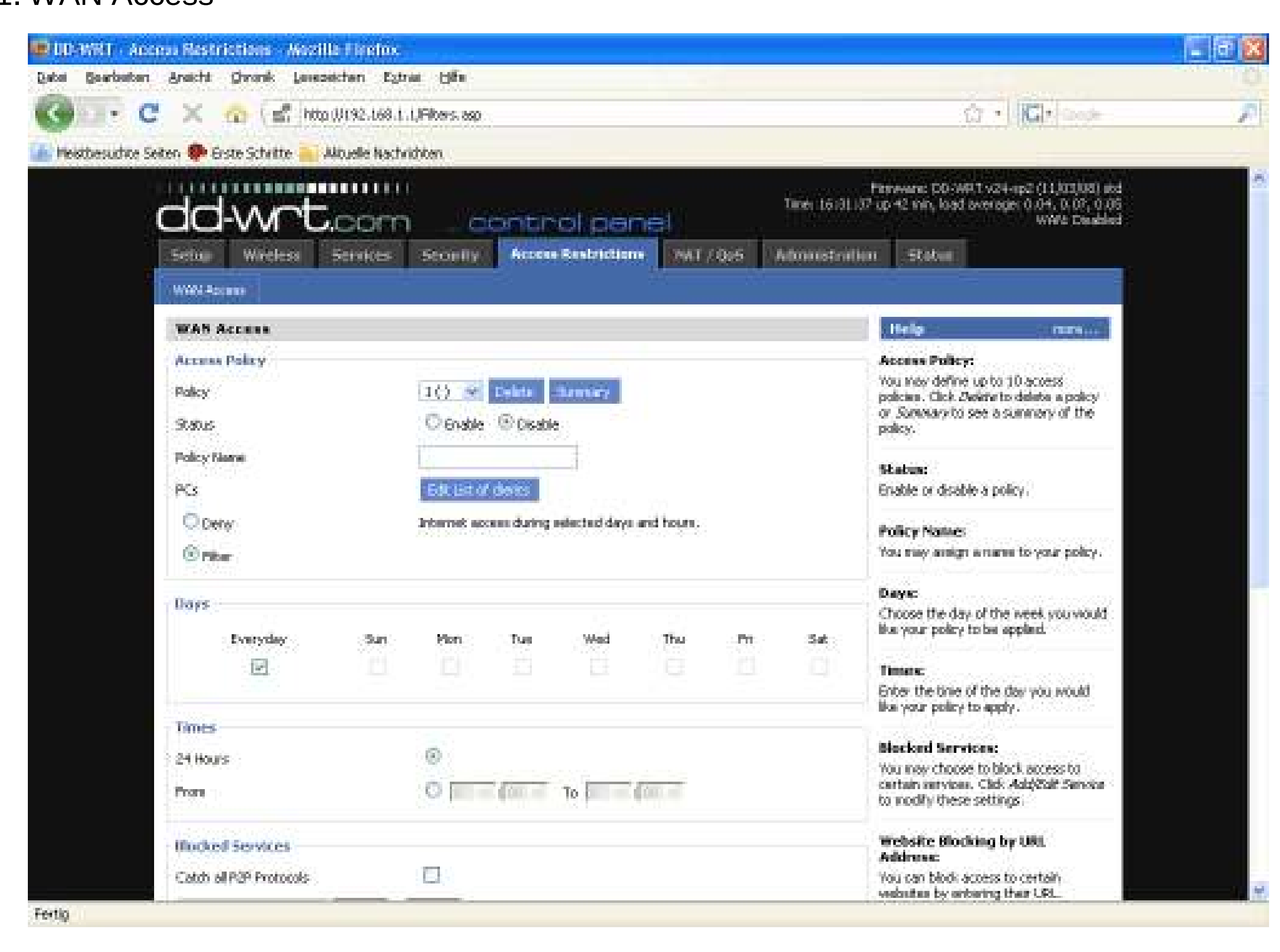
2.3.4.2. VPN



Im VPN-Tab wird das Firewall-Handling von IPSec, PPTP und L2TP-Verbindungen definiert. Standardmäßig ist Passthrough eingestellt.

2.3.5. Access Restrictions

2.3.5.1. WAN Access

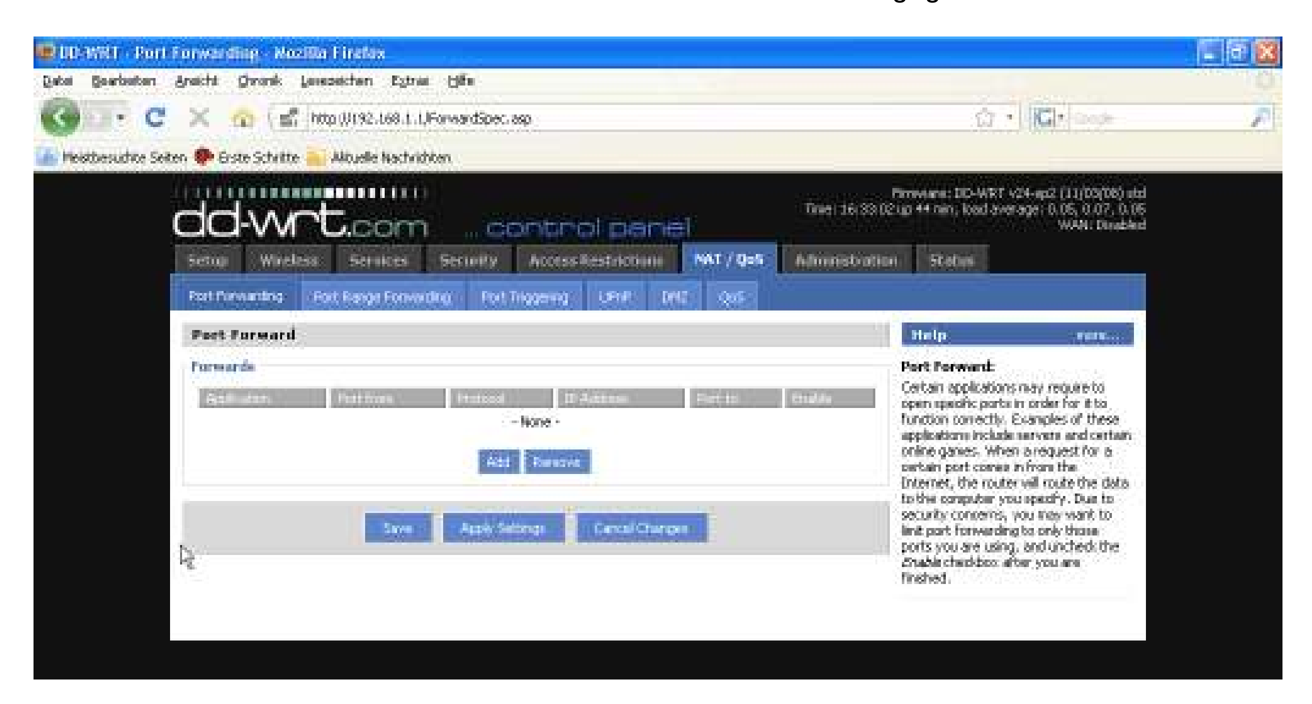


Über diese Einstellungen können Zeit- und Dienste-bezogenen Zugriffsregeln definiert werden.

2.3.6. NAT / QoS

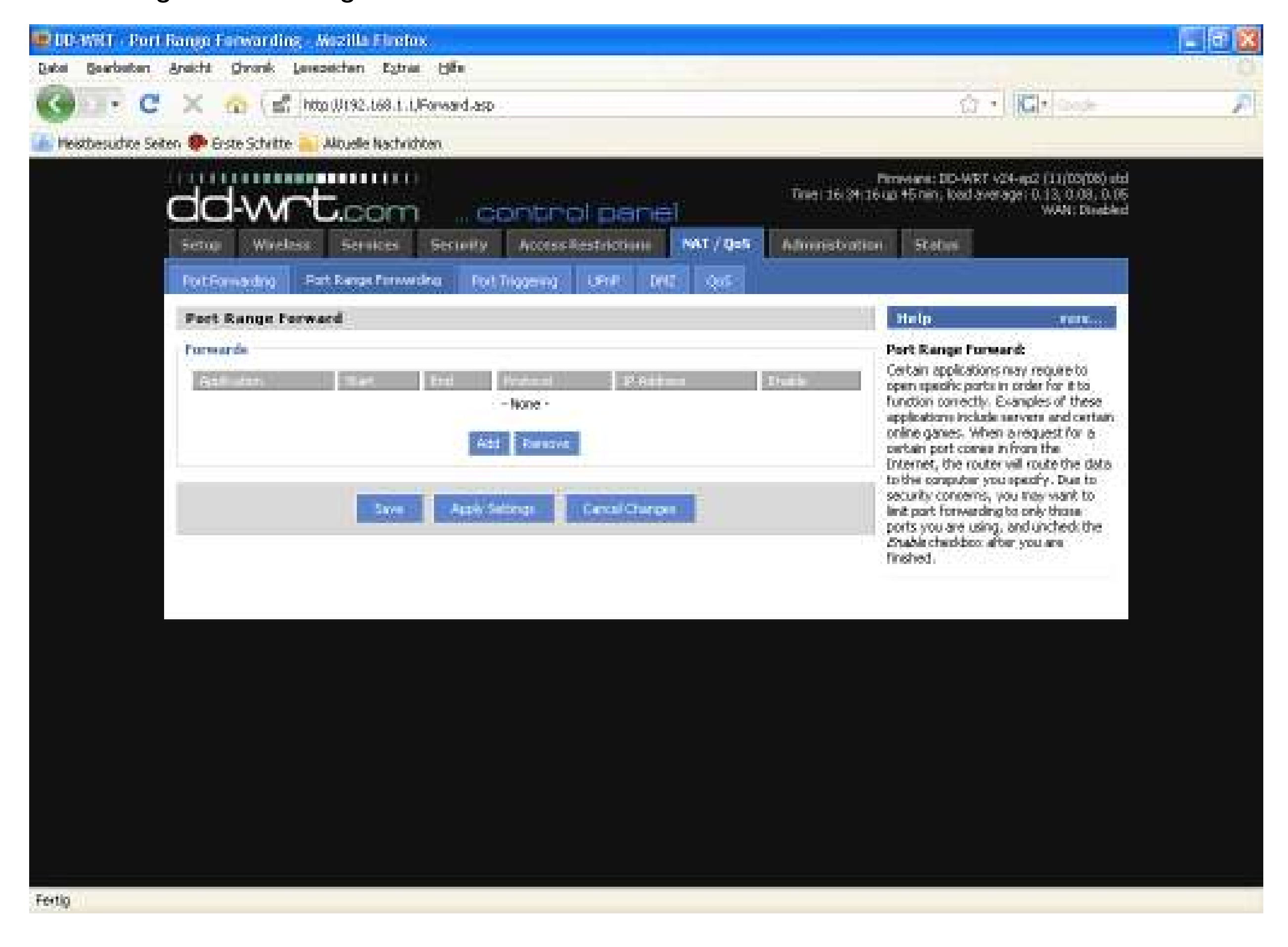
2.3.6.1. Port Forwarding

Port Forwarding erlaubt es Ports vom WAN-Interface bestimmten IP-Adressen und entsprechenden Ports auf internen LAN-Adressen zuzuordnen und so den entsprechenden Datenverkehr von außen nach innen durchleitet. Pro Port Forwarding-Eintrag kann ein Quell-Port sowie eine IP-Adresse und der Ziel-Port für diese Adresse angegeben werden.



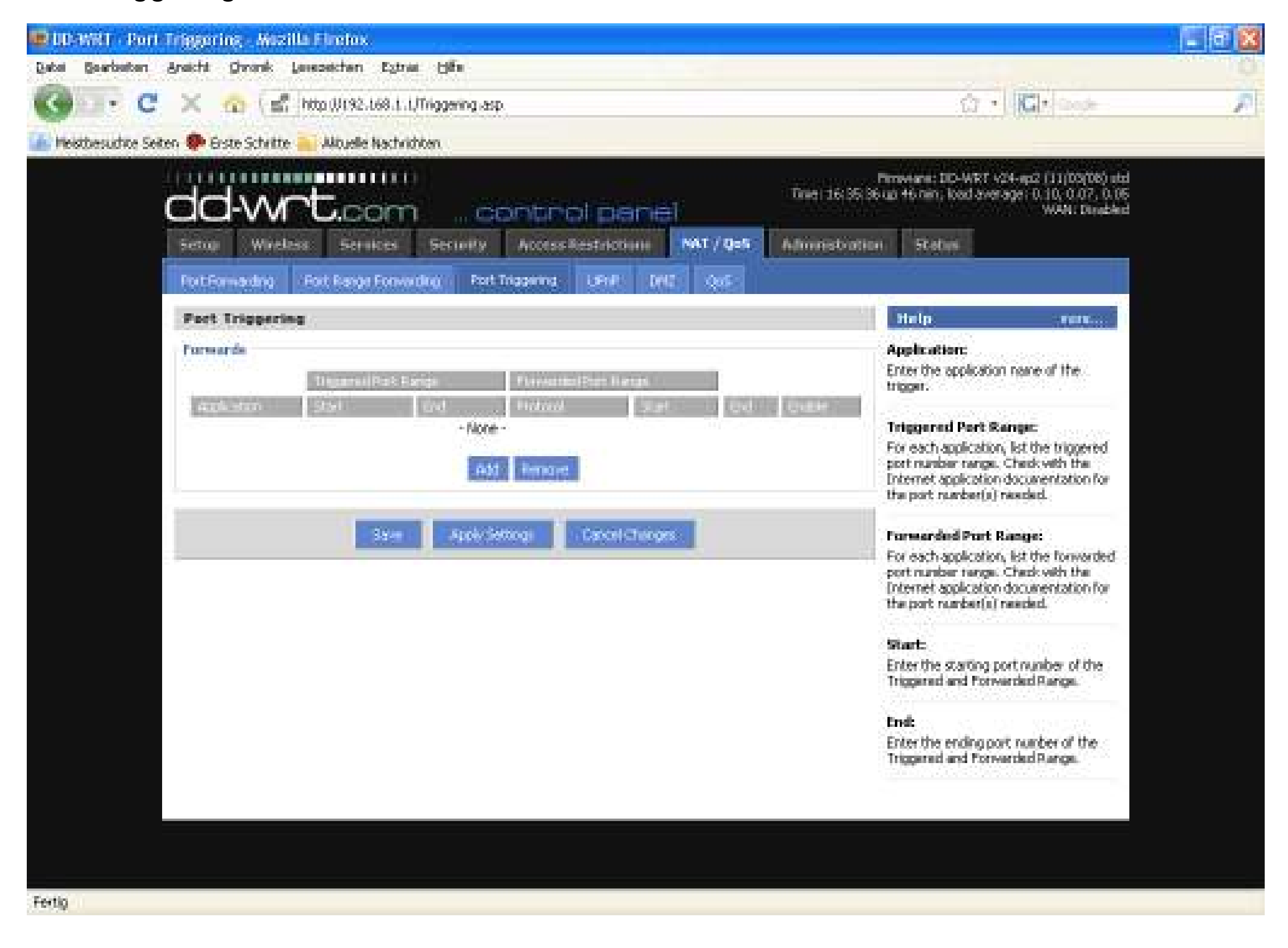
Vor dem Hinzufügen oder dem Entfernen eines neuen Portforwards sollten geänderte Einstellungen gespeichert werden, da die Eingabemaske bei diesen Vorgängen neu geladen werden und nicht gespeicherte Eingaben verloren gehen.

2.3.6.2. Port Range Forwarding



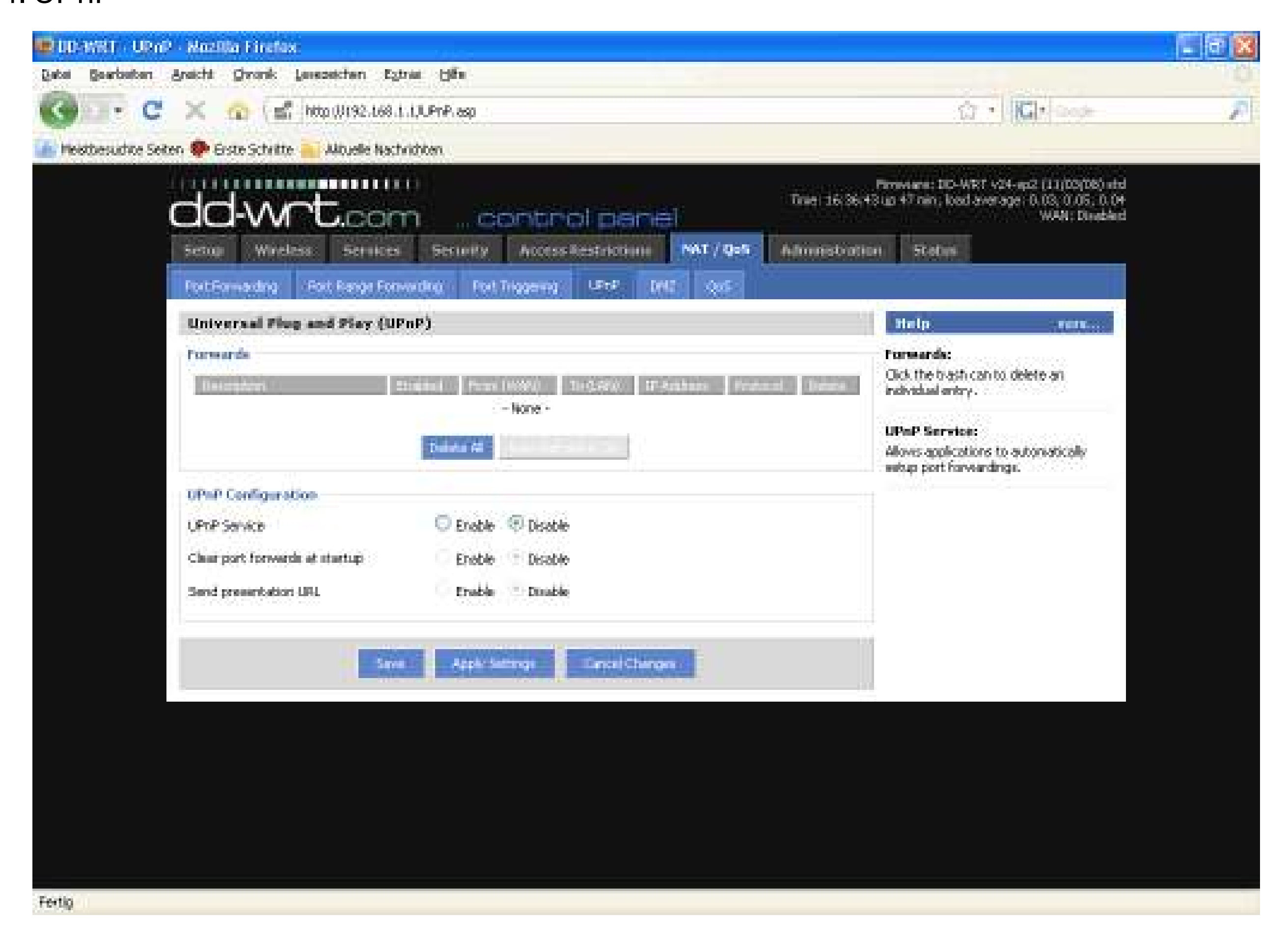
Port Range Forwarding funktioniert ähnlich wie das Port Forwarding. Im Unterschied zu diesem wird beim Port Range Forwarding ein Port-Bereich angegeben, der dann 1 : 1 auf die entsprechenden Ports der internen Ziel-Adresse durchgeleitet werden.

2.3.6.3. Port Triggering



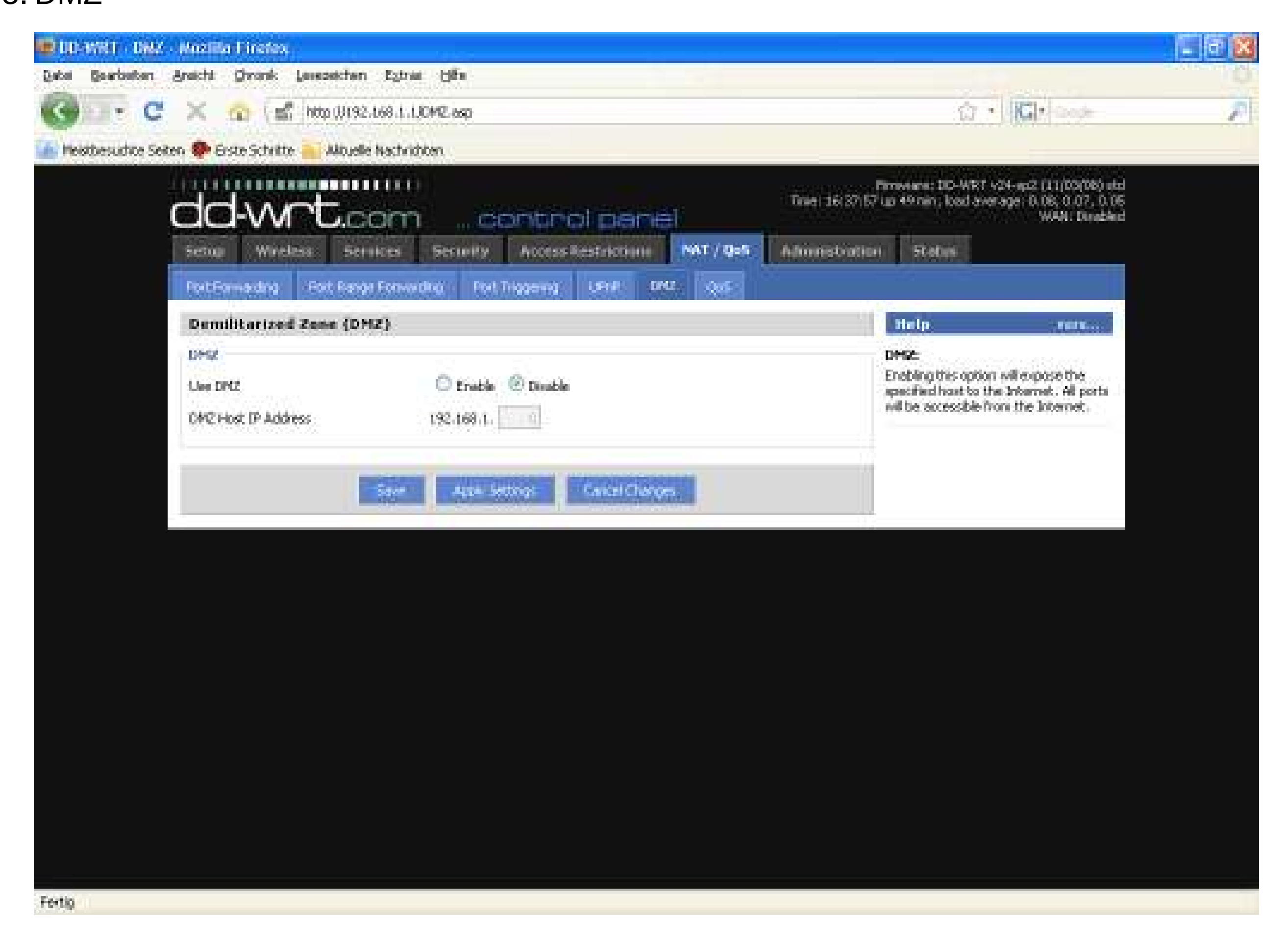
Beim Port Triggering handelt es sich um eine Art Port Range Forwarding, bei dem ausgehender Datenverkehr auf bestimmten Ports wiederum Port Forwards für zuvor definierte Ports des jeweils aktivierenden Rechners aktiviert. Dadurch ist es möglich Ports applikationsbezogen nur temporär zu öffnen und bietet für entsprechende Anwendungsfälle ein höheres Maß an Sicherheit als Port Forwarding bzw. Port Range Forwarding.

2.3.6.4. UPnP



Bei der Nutzung von UPnP können Anwendungen oder Geräte die UPnP-fähig sind die benötigen Ports zum Empfang von Daten automatisch öffnen und auch wieder schließen. Dies erfordert keine weiteren Konfigurationsarbeiten durch den Anwender und ermöglicht ein sehr einfaches Handling.

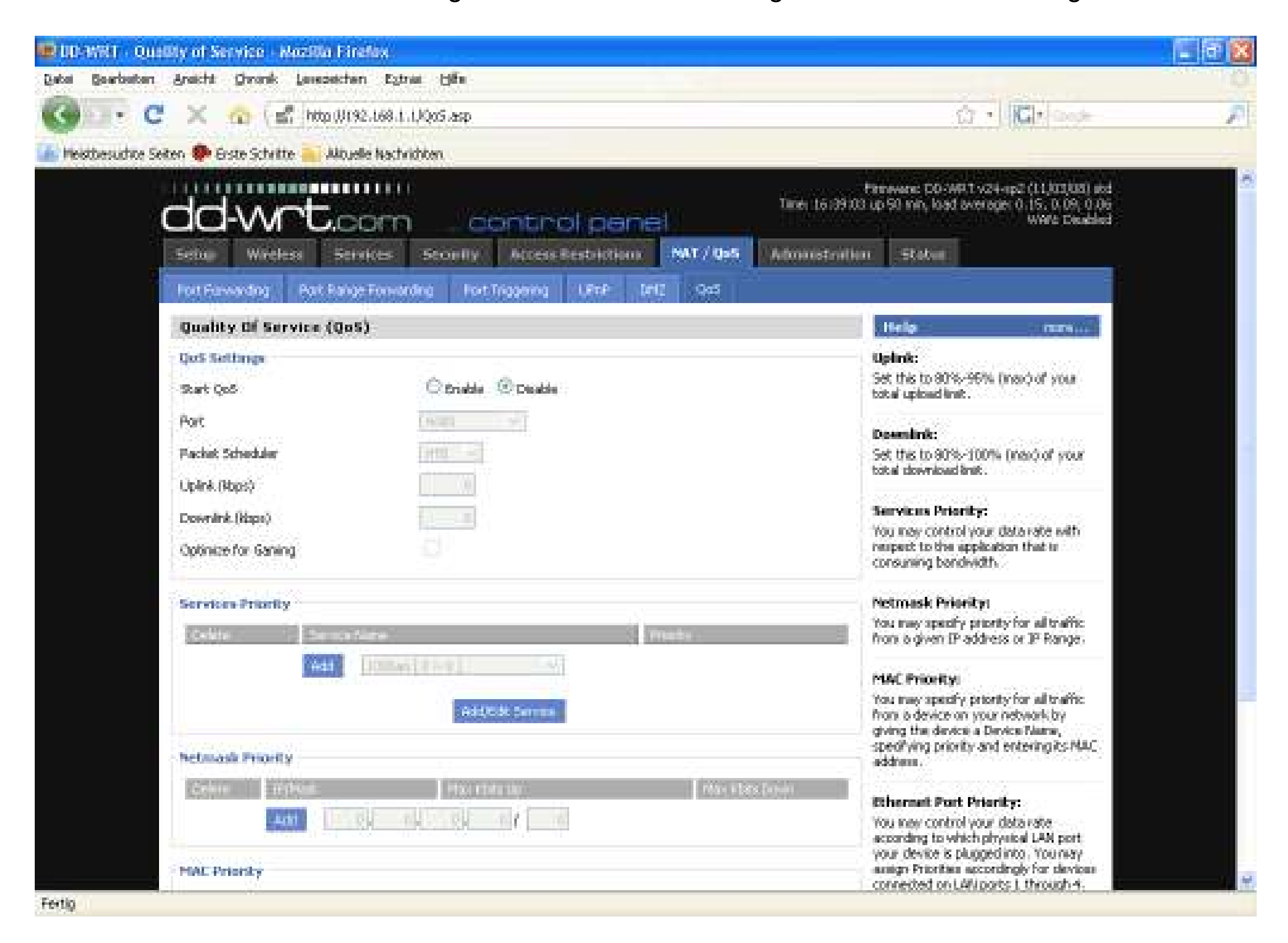
2.3.6.5. DMZ



Ein DMZ-Rechner ist ein spezieller Rechner im internen Netzwerk auf den sämtlicher eingehender Netzwerkverkehr weitergeleitet wird. Die Aufgabe eines solchen Rechner ist es, diesen Datenverkehr entsprechend zu managen. Wenn die DMZ-Funktion aktiviert ist, wird die interne Firewall deaktiviert, was bei nachlässiger Konfiguration ein Sicherheitsrisiko darstellen kann. Des weiteren funktionieren verschiedene Dienste des Routers, die von Außen erreichbar sein müssen, nicht mehr, da der entsprechende Datenverkehr ebenfalls auf den DMZ-Rechner weitergeleitet wird.

2.3.6.6. QoS

QoS (Quality of Service) ist ein Verfahren, Datenverkehr applikationsbezogen zu priorisieren und so bestimmten Diensten möglichst die minimal benötigte Bandbreite zu ermöglichen.

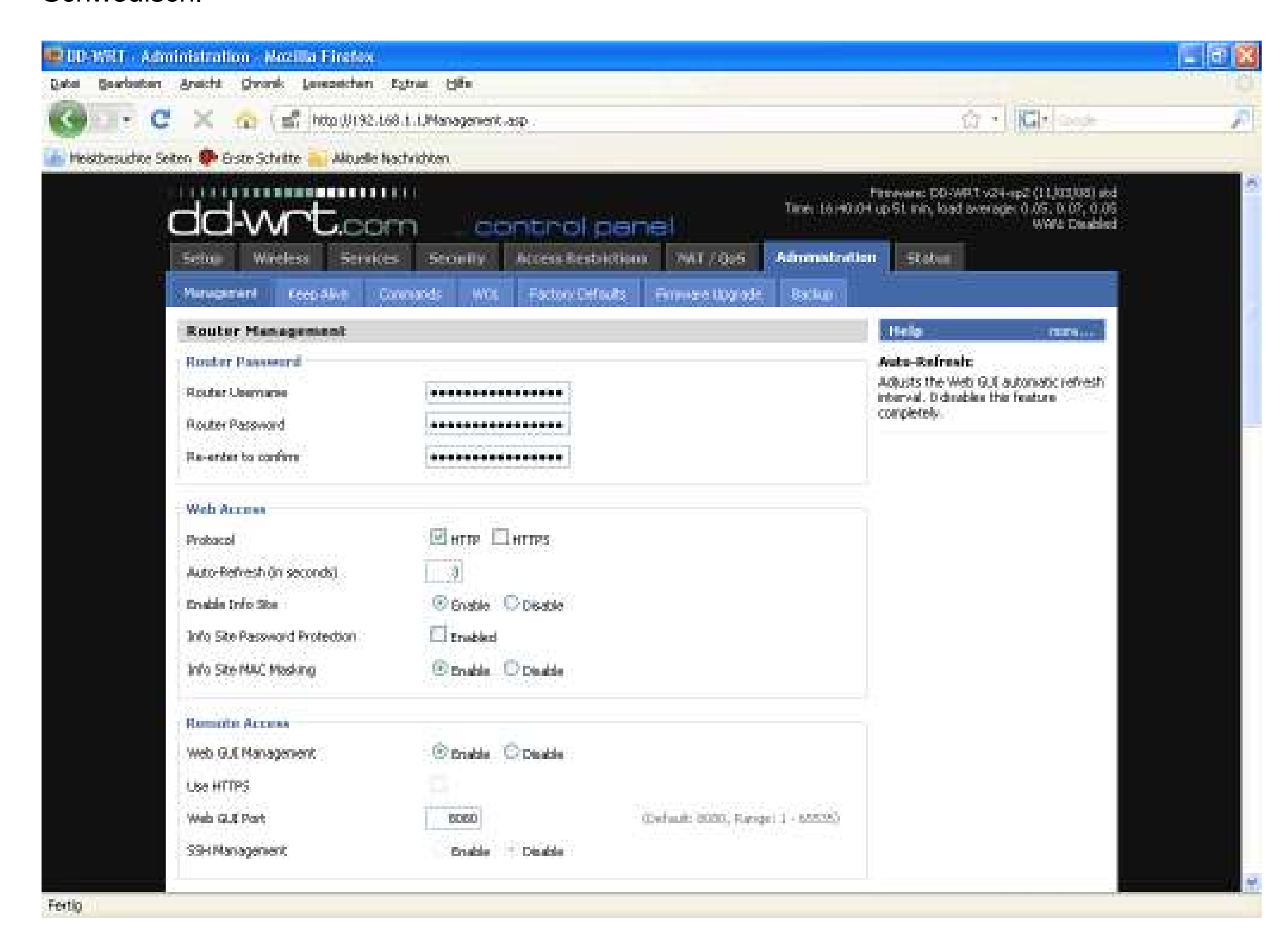


Die Einstellungen im Bereich QoS erlauben es, neben der generellen Bandbreite für Up- und Downstream auch Einstellungen für bestimmte Dienste und IP-Adressbereiche sowie MAC-Adressen vorzunehmen.

2.3.7. Administration

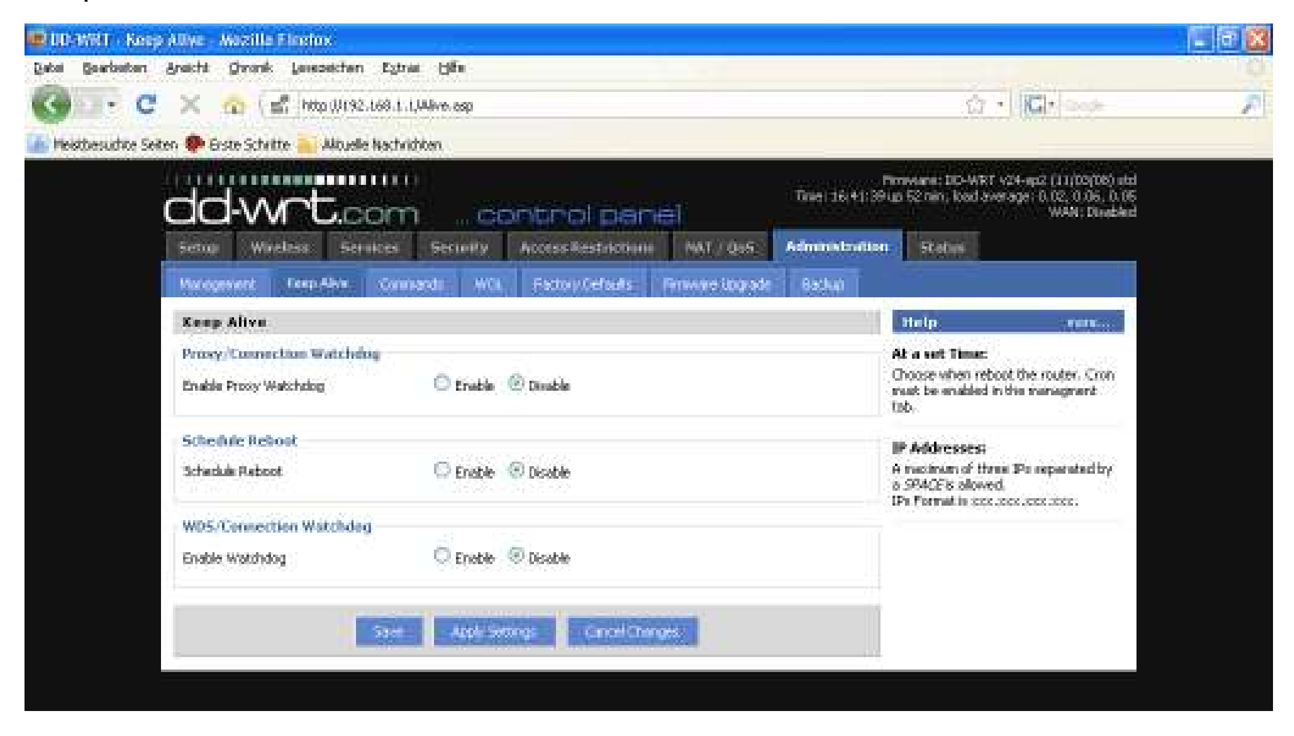
2.3.7.1. Management

Hier finden sich alle notwendigen Einstellungen für den Management-Zugriff auf den Router sowie weitere seltener benötigte Grundeinstellungen. Des weiteren kann hier die Interface-Sprache für das Web-GUI eingestellt werden (Standard Englisch), zur Auswahl stehen Chinesisch (vereinfacht oder traditionell), Niederländisch, Englisch, Französisch, Deutsch, Ungarisch, Italienisch, Japanisch, Polnisch, Portugiesisch, Slowenisch, Spanisch und Schwedisch.



Für die Remote-Administration notwendige Systemdienste wie Telnet oder SSH müssen im Bereich „Services“ erst aktiviert werden, bevor die zugehörigen Einstellungen vorgenommen werden können.

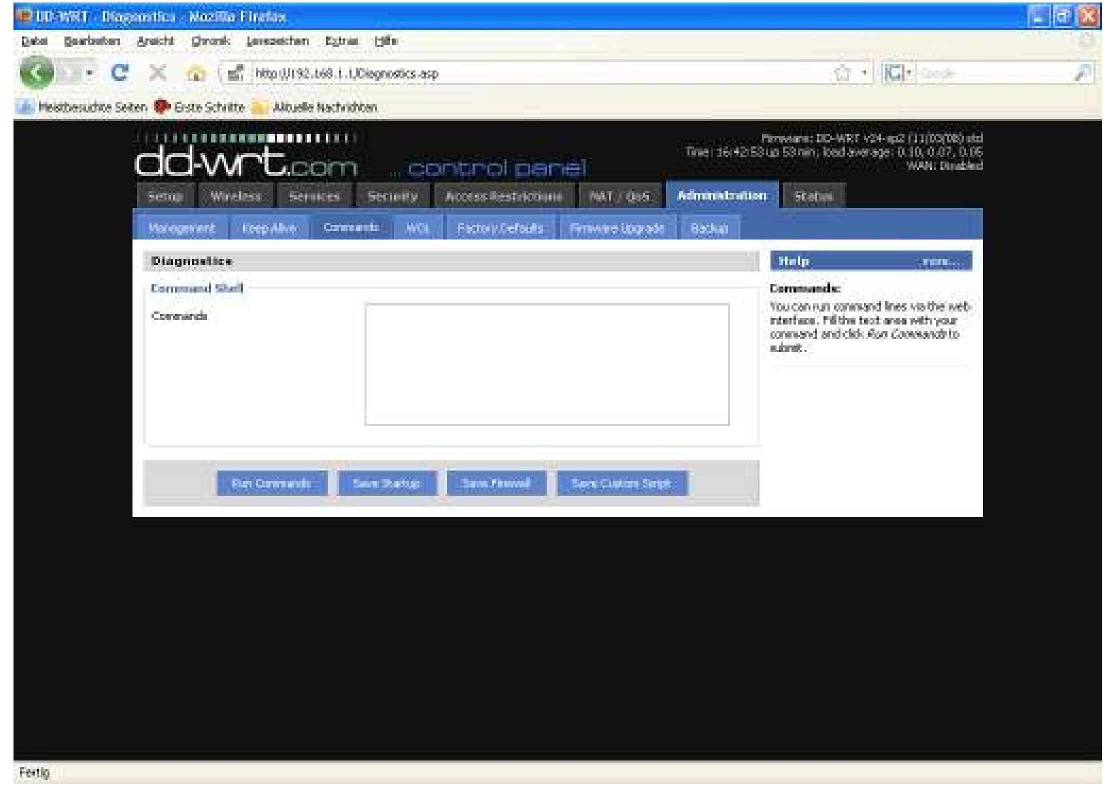
2.3.7.2. Keep Alive



Die Keep-Alive Funktionalität ermöglicht es, verschiedene Überwachungsmethoden zu aktivieren, die bei einer möglichen Funktionsstörung das System neu starten.

2.3.7.3. Commands

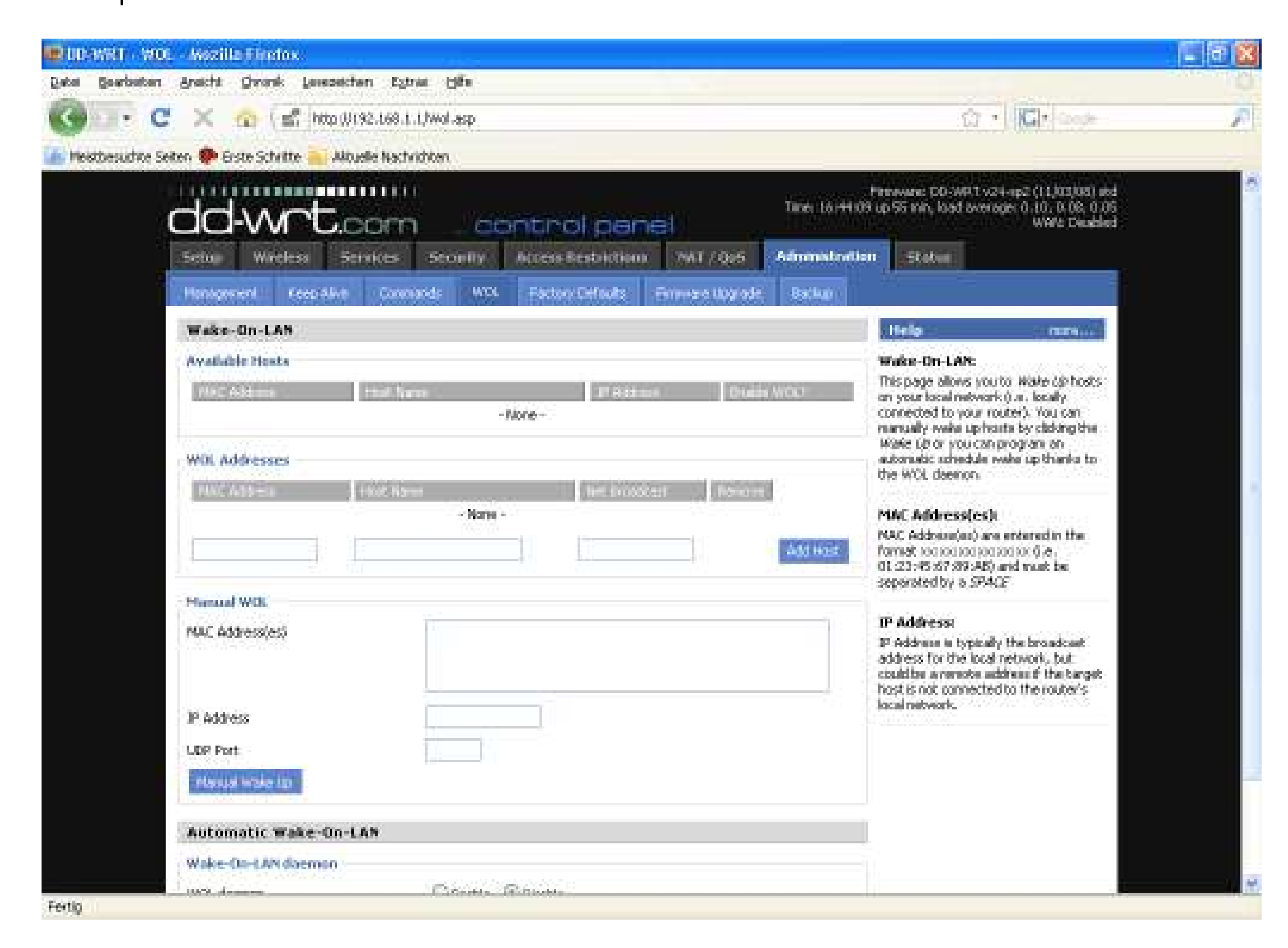
Hier können verschiedene Linux-Kommandozeilen-Aktionen ausgeführt werden um Einstellungen vorzunehmen, die direkt über das WebGUI nicht oder nicht in der gewünschten Art möglich sind. Es handelt sich hier um ein sehr mächtiges Werkzeug, dass aber mit Bedacht verwendet werden sollte, da falsche Eingaben den Router in einen nicht funktionsfähigen Zustand versetzen können.



Neben dem direkten Ausführen von Shell-Kommandos können auch Startskripte und Firewall-Scripte hinterlegt werden, das Speichern eigener Shell-Scripte ist ebenfalls möglich.

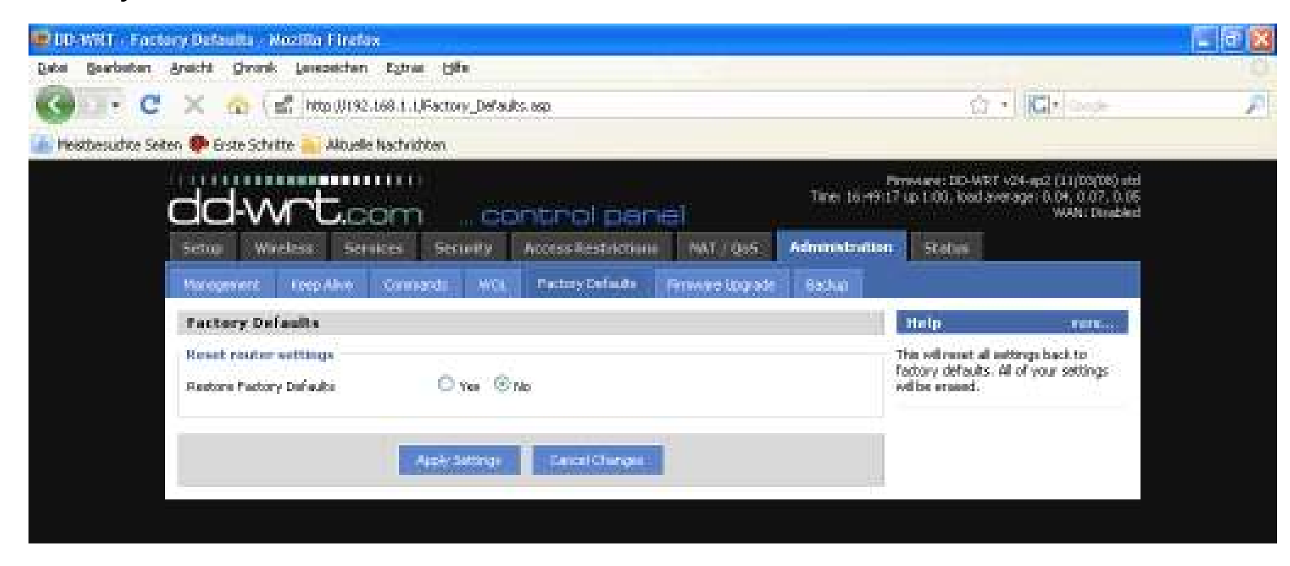
2.3.7.4. WOL

„Wakeup On LAN“ erlaubt es, entsprechend konfigurierte Rechner im Netzwerk über ein WOL-Datenpaket zu starten.



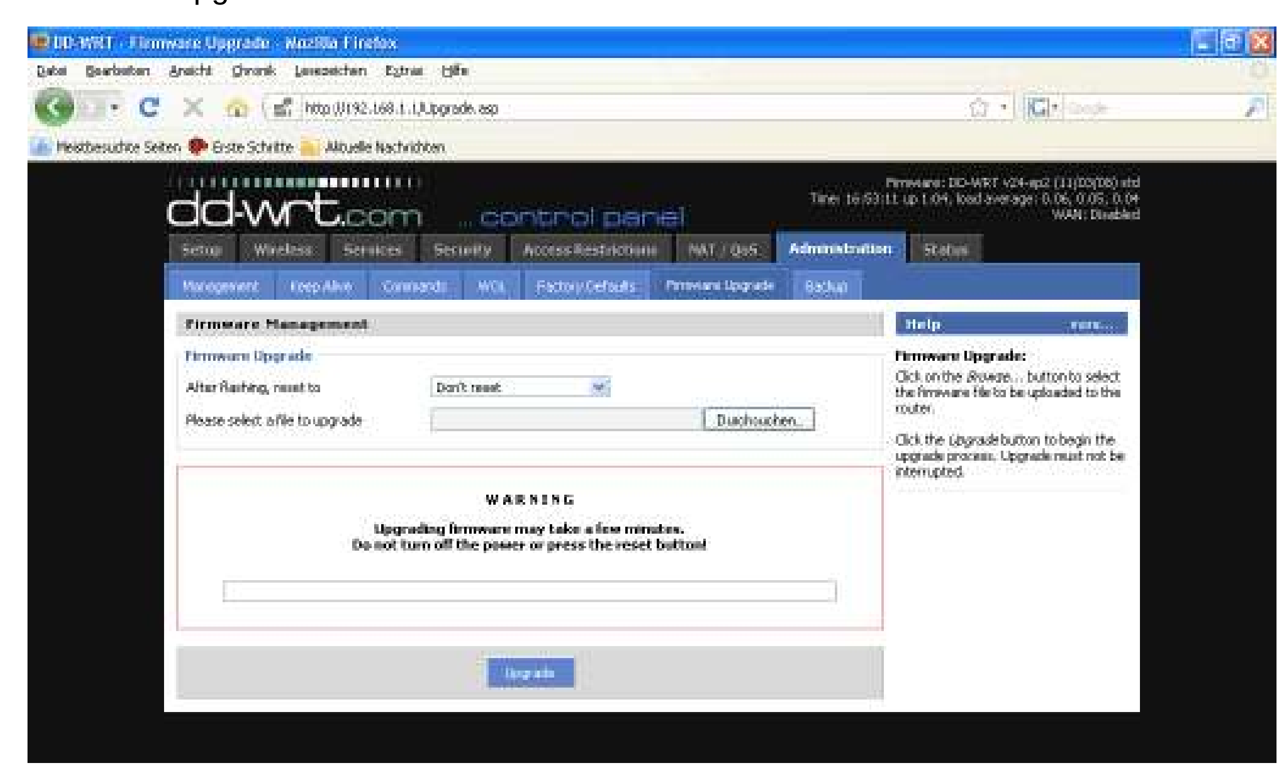
Die WOL-Pakete können entweder manuell oder automatisch zu einer bestimmten Zeit verschickt werden.

2.3.7.5. Factory Defaults



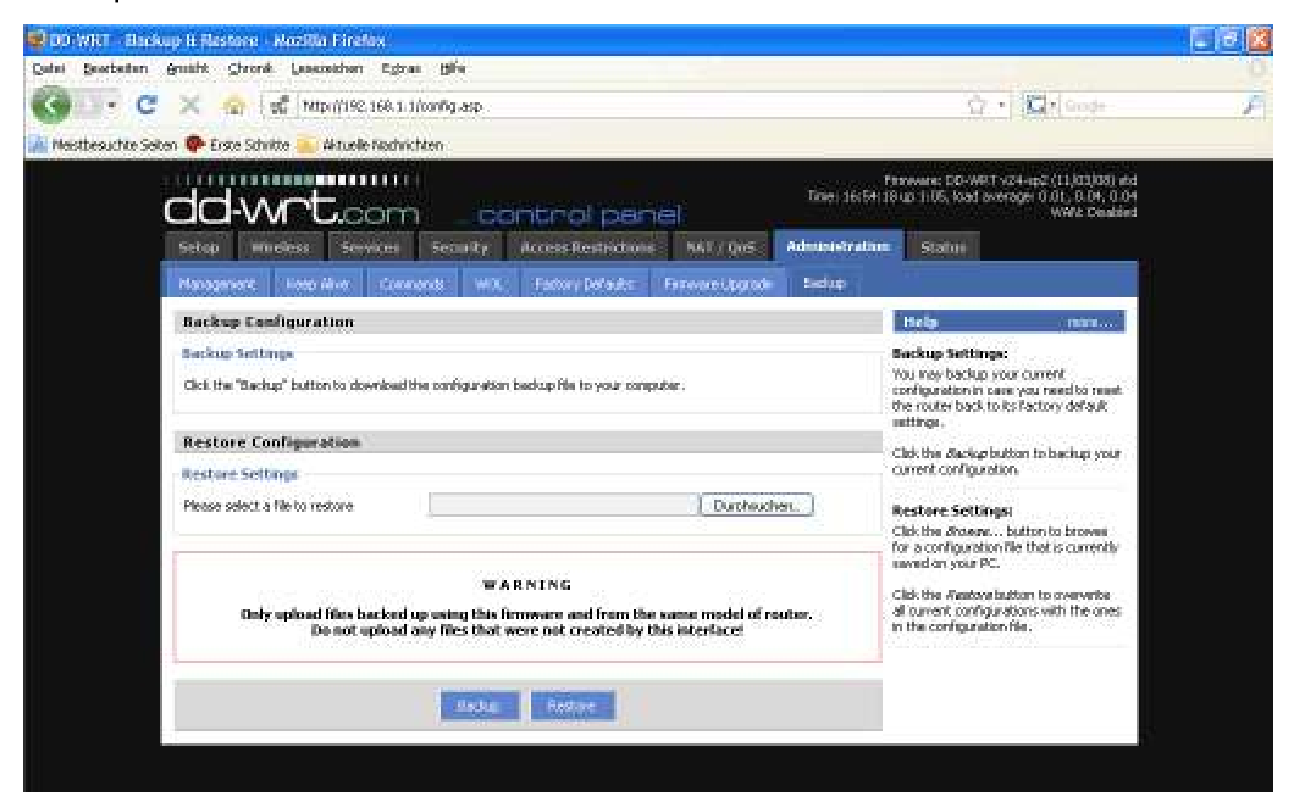
Über diese Funktion kann der Router auf die Auslierungseinstellungen zurückgesetzt werden. Der Router führt nach dem Zurücksetzen einen Neustart durch.

2.3.7.6. Firmware Upgrade



Mit Hilfe der Firmware Upgrade Funktion können neue Versionen der Firmware eingespielt werden. Dabei kann gewählt werden, ob die Einstellungen zurückgesetzt werden sollen oder nicht.

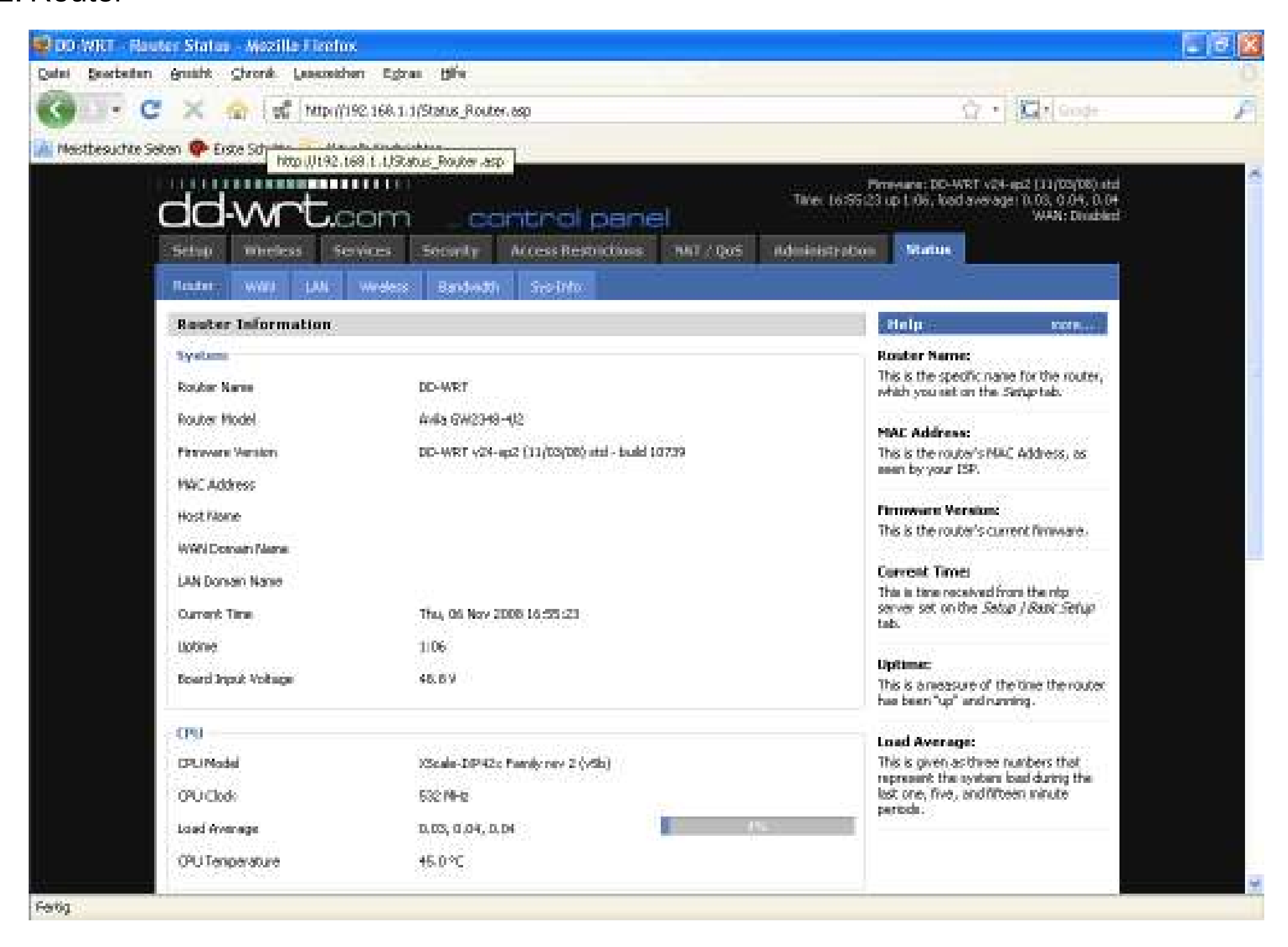
2.3.7.7. Backup



Der Menüpunkt „Backup“ beinhaltet die Funktionen zum Sichern und Zurückspielen einer Routerkonfiguration. Dies kann zu Backup-Zwecken oder für das Aufsetzen verschiedener Router mit gleichen / ähnlichen Einstellungen benutzt werden.

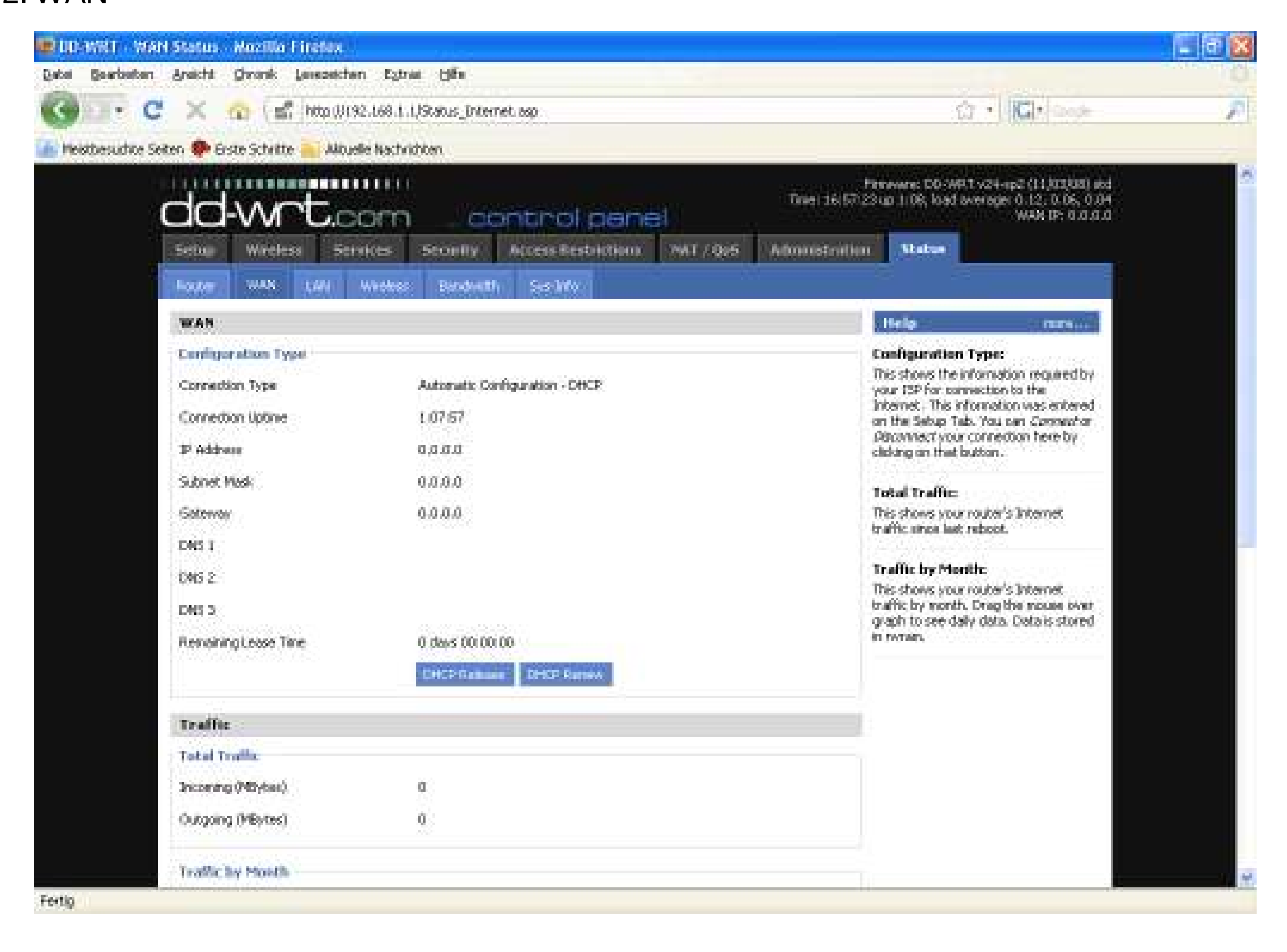
2.3.8. Status

2.3.8.1. Router



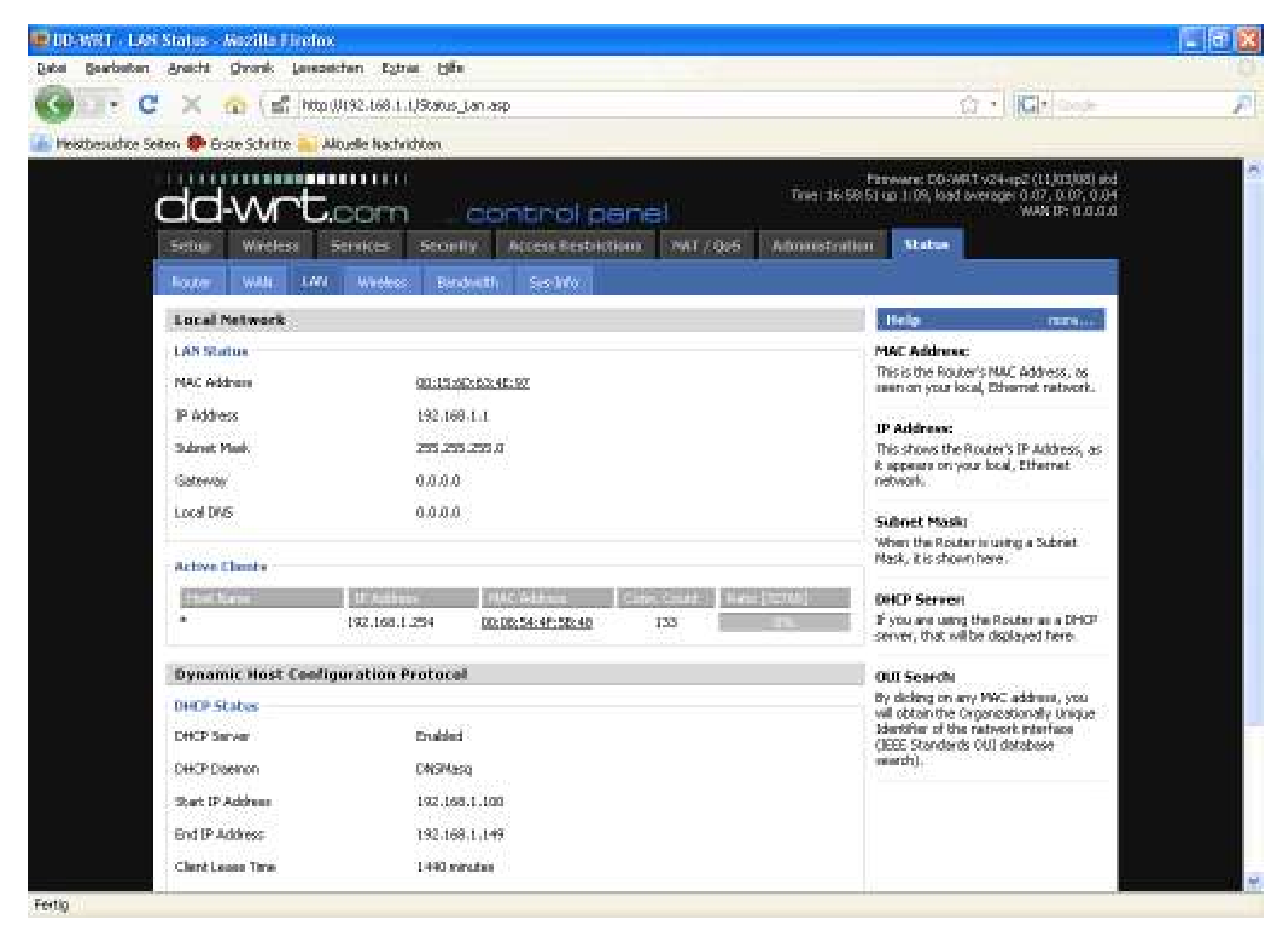
Hier findet man allgemeine Informationen über den Router wie Systemlast, Speichernutzung und aktuell aktive IP-Verbindungen.

2.3.8.2. WAN



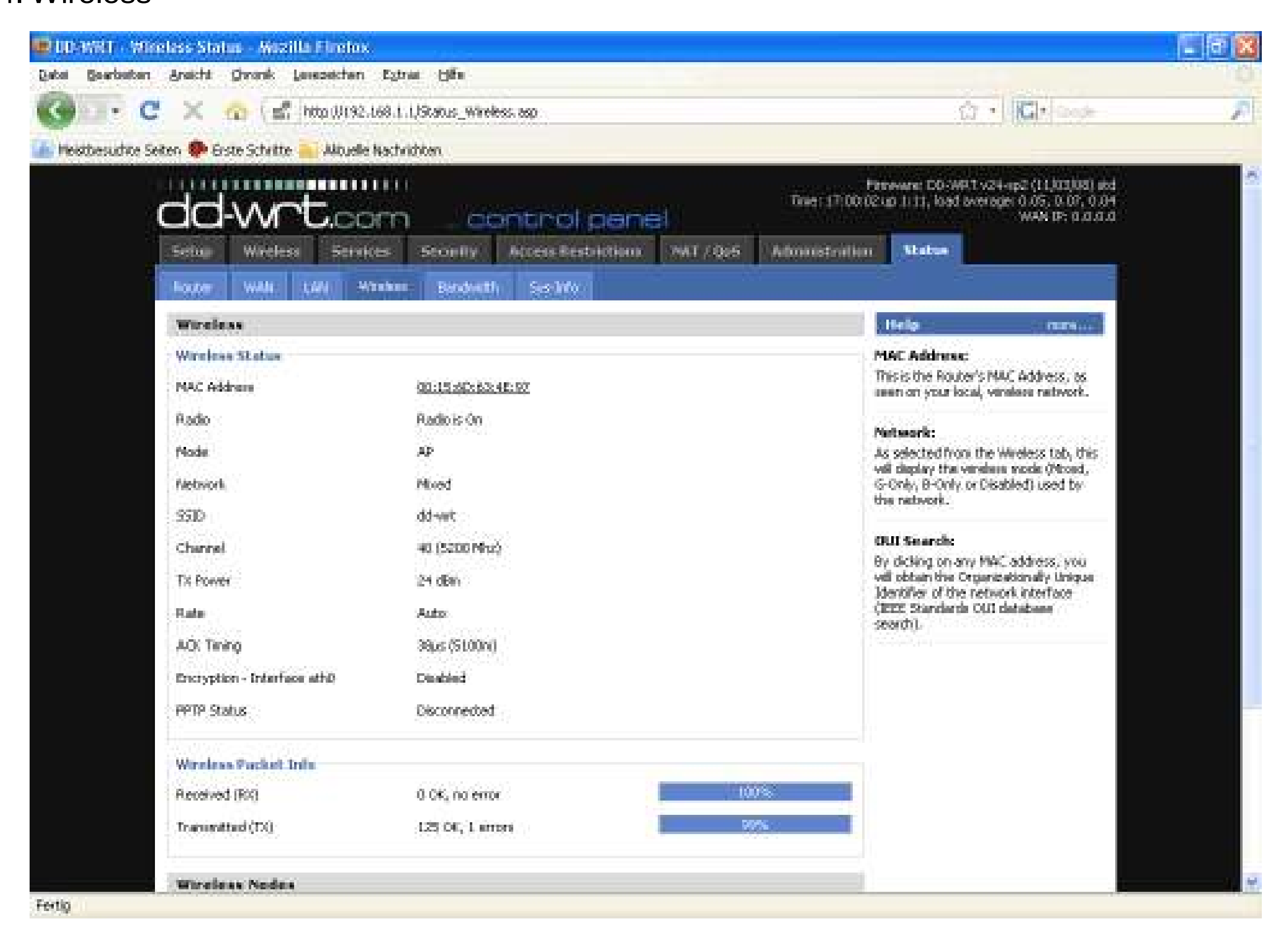
Sofern das WAN-Inferface aktiv ist, werden hier die relevanten WAN-Einstellungen und Datendurchsatzstatistiken angezeigt.

2.3.8.3. LAN



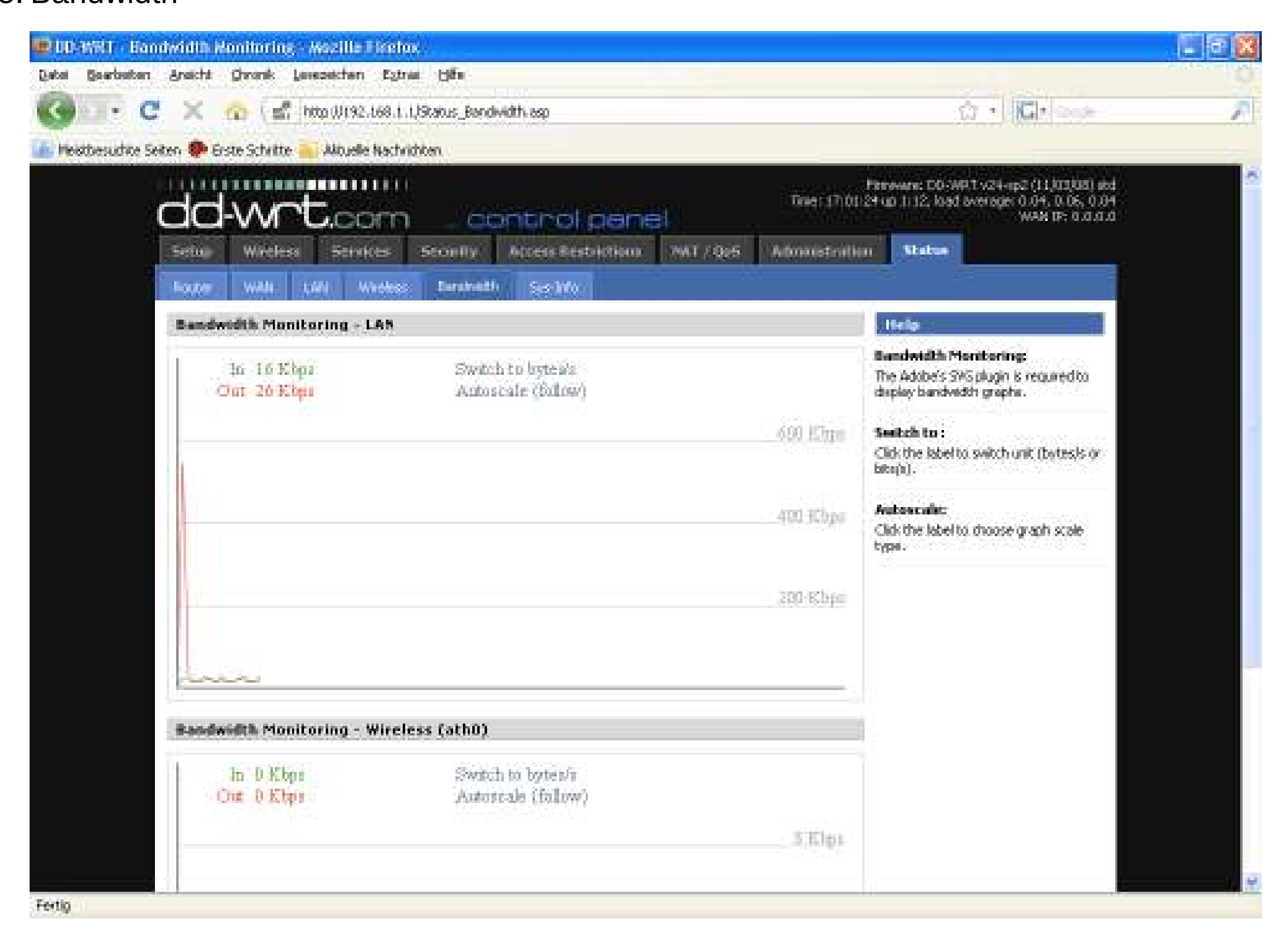
Diese Übersicht zeigt die für das LAN relevanten Informationen wie aktive Clients und die DHCP-Clients an.

2.3.8.4. Wireless



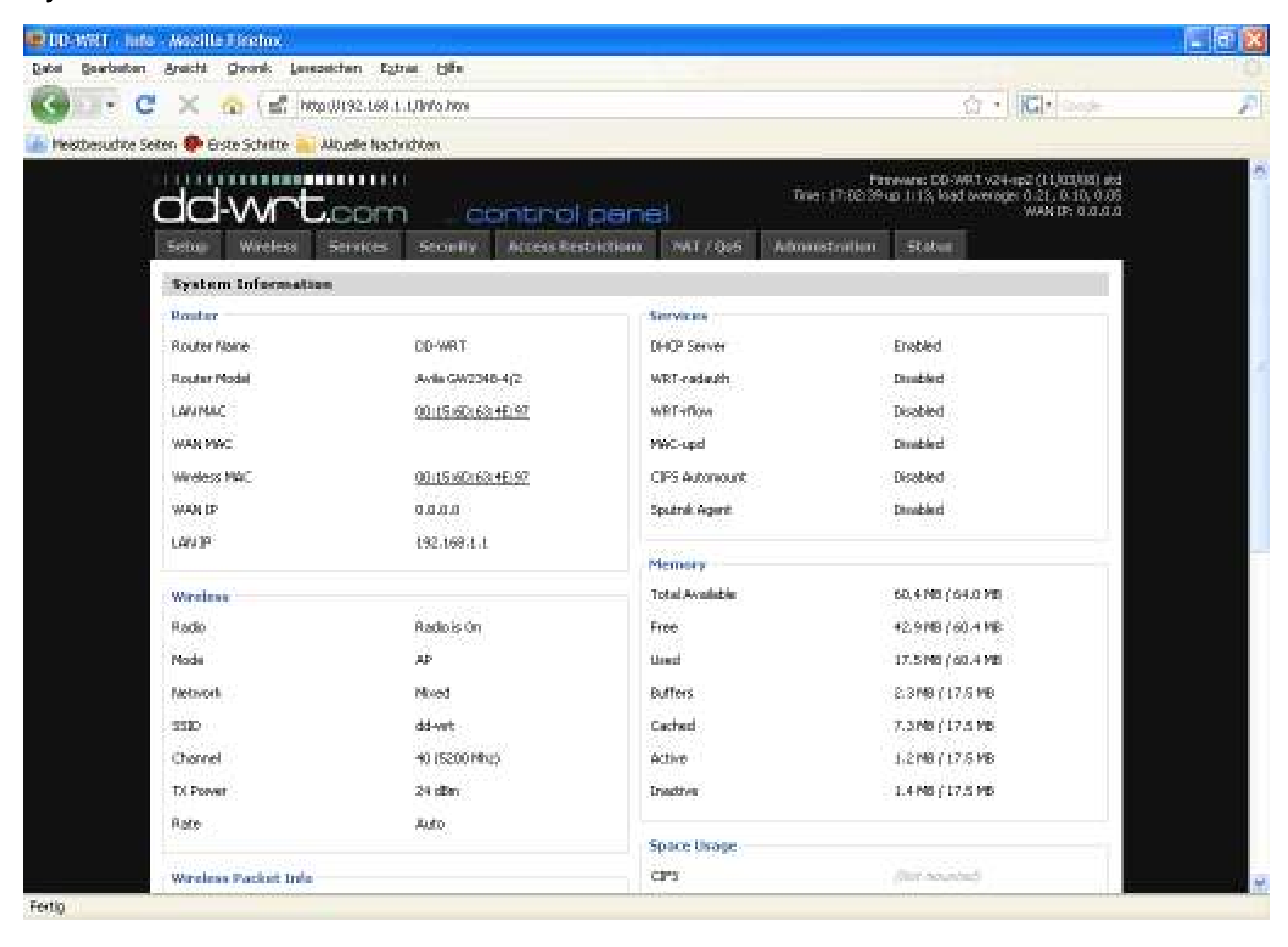
Hier wird der Status der Wireless Interfaces und die aktiven Wireless Verbindungen angezeigt. Sofern mehrere Wireless Interfaces im System vorhanden sind, kann zwischen diesen über das PullDown-Menü im Wireless Status umgeschaltet werden.

2.3.8.5. Bandwidth



In diesem Bereich wird der Ein-/Ausgehende Datenverkehr für jedes Netzwerk-Interface angezeigt.

2.3.8.6. SysInfo



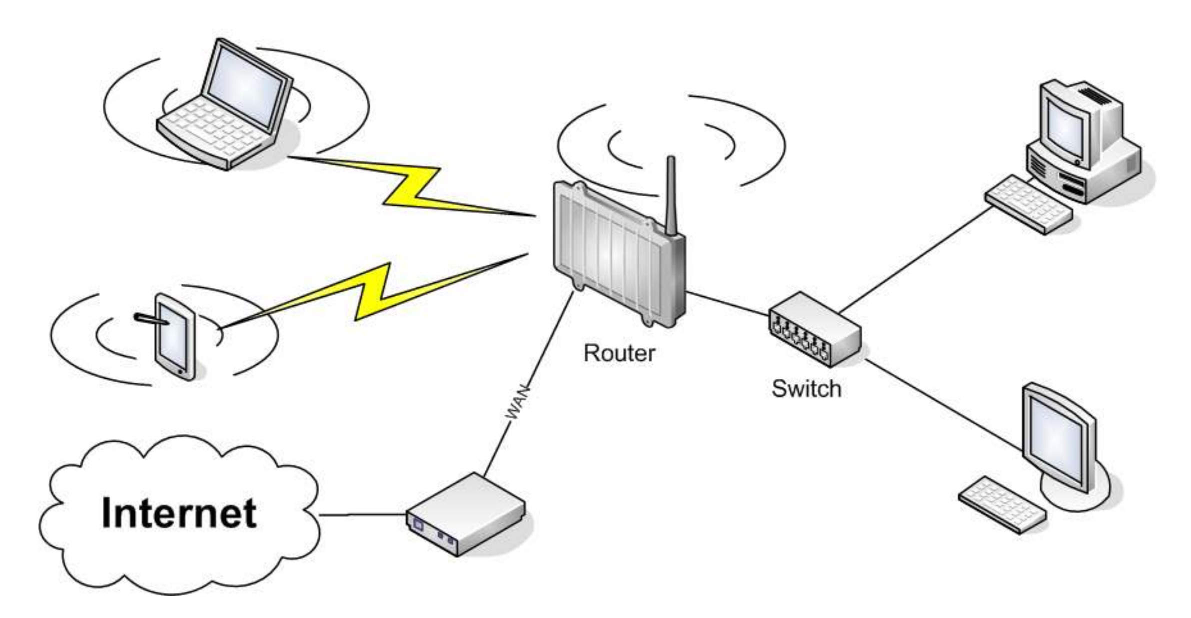
Unter SysInfo sind die wichtigsten Informationen der verschiedenen Statusseiten zusammengefasst. Es ist zu beachten, dass die Systeminformations-Seite standardmäßig ohne Passwortabfrage zugänglich ist. Dies kann über die entsprechenden Einstellungen im Management-Bereich der Administration so geändert werden, dass dieses Seite entweder gar nicht oder nur per Passwort-Abfrage zugänglich ist.

3. Anwendungsbeispiele

Die folgenden Anwendungsbeispiele beziehen sich auf die häufigsten Anwendungsfälle und bieten schrittweise Instruktionen für die Konfiguration.

3.1. Access Point

Access Point (AP, manchmal auch als Infrastructure Mode bezeichnet) beschreibt die Konfiguration eines Routers als zentrale Netzwerkkomponente, bei der drahtloses oder drahtgebundene Geräte über den Router aufeinander und auf Geräte in anderen Netzen (z.B. im Internet) zugreifen können.



Verbinden Sie Ihren Rechner mit dem Router wie unter 2.1. beschrieben und greifen Sie auf das Webinterface wie unter 2.2. beschrieben zu.

3.1.1. Access Point mit NAT / DHCP

Setup -> Basic Setup

- *WAN Setup*
  - Wählen Sie bei „Connection Type“ die Art der WAN-Anbindung und nehmen Sie die jeweiligen Einstellungen vor
- *Network Setup*
  - Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - Setzen Sie „DHCP Type“ auf „DHCP Server“ (sofern nicht gesetzt)
  - Setzen Sie „DHCP Server“ auf „Enable“ (sofern nicht gesetzt)
  - Passen Sie ggf. den DHCP-Adressbereich an, den der Server vergeben soll
- *Time Settings*
  - Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „AP“
- Stellen Sie bei „Wireless Network Mode“ den gewünschten Modus ein, beachten Sie, dass der gemischte Betrieb (BG-Mixed) von 802.11b und 802.11g (2,4 GHz) zu Performanceeinbußen führt
- Setzen Sie die „Wireless Network Name (SSID)“ auf den gewünschten Netzwerknamen
- Klicken Sie auf „Save“

Wireless -> Wireless Security

- Wählen und konfigurieren Sie den gewünschten Sicherheitsmodus (Beachten Sie, dass WEP konzeptionell unsicher ist und nur verwendet werden sollte, wenn dies absolut unabdingbar ist)
- Klicken Sie auf „Apply Settings“

Sie können nun den Router über das LAN-Interface mit dem Internet / Ihrem Netzwerk verbinden. Wenn Sie Geräte per WLAN mit dem Router verbinden, sollten diese nach erfolgreichem Verbindungsaufbau im Statusbereich als DHCP- und WLAN-Clients aufgeführt werden.

3.1.1. Access Point hinter einem Netzwerk / Internet Gateway

Setup -> Basic Setup

- *WAN Setup*
  - Wählen Sie bei „Connection Type“ die Einstellung „Disabled“
- *Network Setup*
  - Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - Setzen Sie „DHCP Type“ auf „DHCP Server“ (sofern nicht gesetzt)
  - Setzen Sie „DHCP Server“ auf „Disable“
- *Time Settings*
  - Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „AP“
- Stellen Sie bei „Wireless Network Mode“ den gewünschten Modus ein, beachten Sie, dass der gemischte Betrieb (BG-Mixed) von 802.11b und 802.11g (2,4 GHz) zu Performanceeinbußen führt
- Setzen Sie die „Wireless Network Name (SSID)“ auf den gewünschten Netzwerknamen
- Klicken Sie auf „Save“

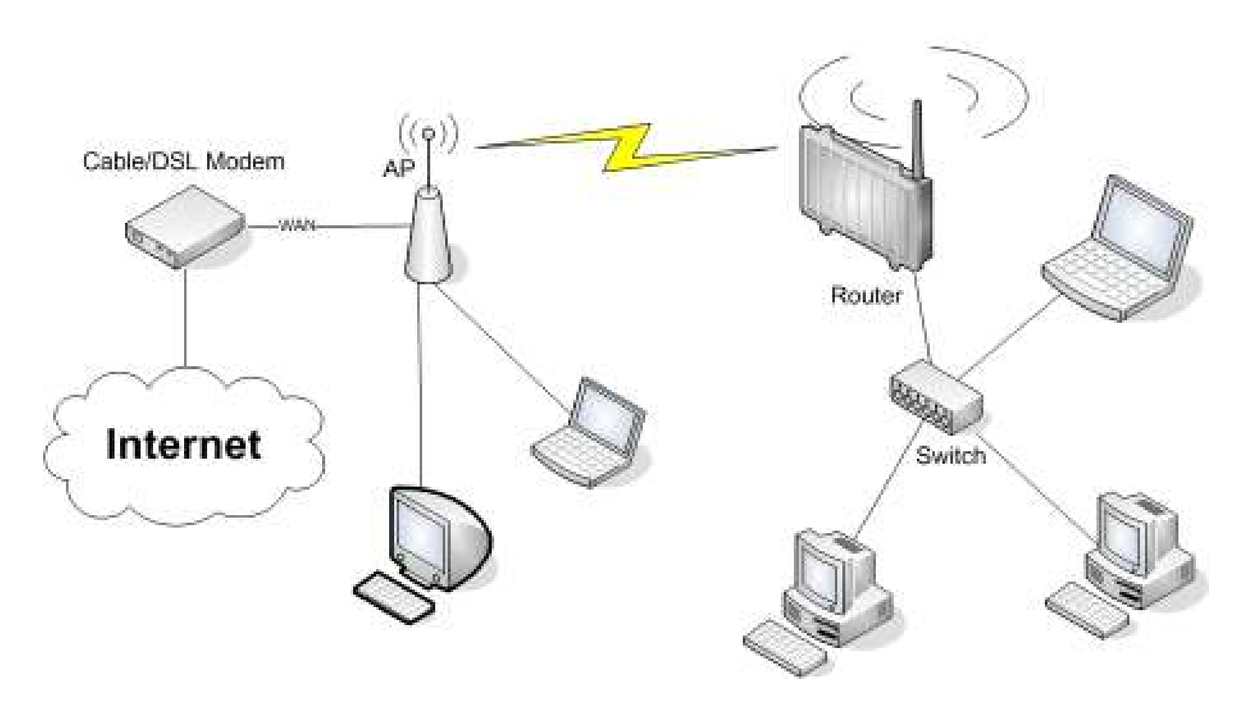
Wireless -> Wireless Security

- Wählen und konfigurieren Sie den gewünschten Sicherheitsmodus (Beachten Sie, dass WEP konzeptionell unsicher ist und nur verwendet werden sollte, wenn dies absolut unabdingbar ist)
- Klicken Sie auf „Apply Settings“

Sie können nun den Router über das LAN-Interface mit dem Internet / Ihrem Netzwerk verbinden. Wenn Sie im LAN einen DHCP-Server betreiben, sollten die per WLAN angeschlossenen Rechner von diesem eine IP-Adresse zugewiesen bekommen.

3.2. Wireless Client

Der Wireless Client Modus kann verwendet werden, eines der WLAN-Interfaces an einen anderen Access Point anzubinden. Das entsprechende WLAN Interface fungiert hierbei als WAN Interface, sodass auf dem Router wiederum ein internes LAN verwendet werden kann.



Setup -> Basic Setup

- *WAN Setup*
  - Stellen Sie bei „Connection Type“ entweder „Static IP“ (falls auf der Seite des AP kein DHCP Server läuft) oder „DHCP“ ein
- *Network Setup*
  - Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - Setzen Sie „DHCP Type“ auf „DHCP Server“ (sofern nicht gesetzt)
  - Setzen Sie „DHCP Server“ auf „Enable“ (sofern nicht gesetzt)
  - Passen Sie ggf. den DHCP-Adressbereich an, den der Server vergeben soll *Time Settings*
- *Time Settings*
  - Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „Client“
- Stellen Sie bei „Wireless Network Mode“ den Modus des Access Points ein, mit dem sich der Router verbinden soll
- Setzen Sie die „Wireless Network Name (SSID)“ auf den für den Access Point konfigurierten Netzwerknamen
- Klicken Sie auf „Save“

Wireless -> Wireless Security

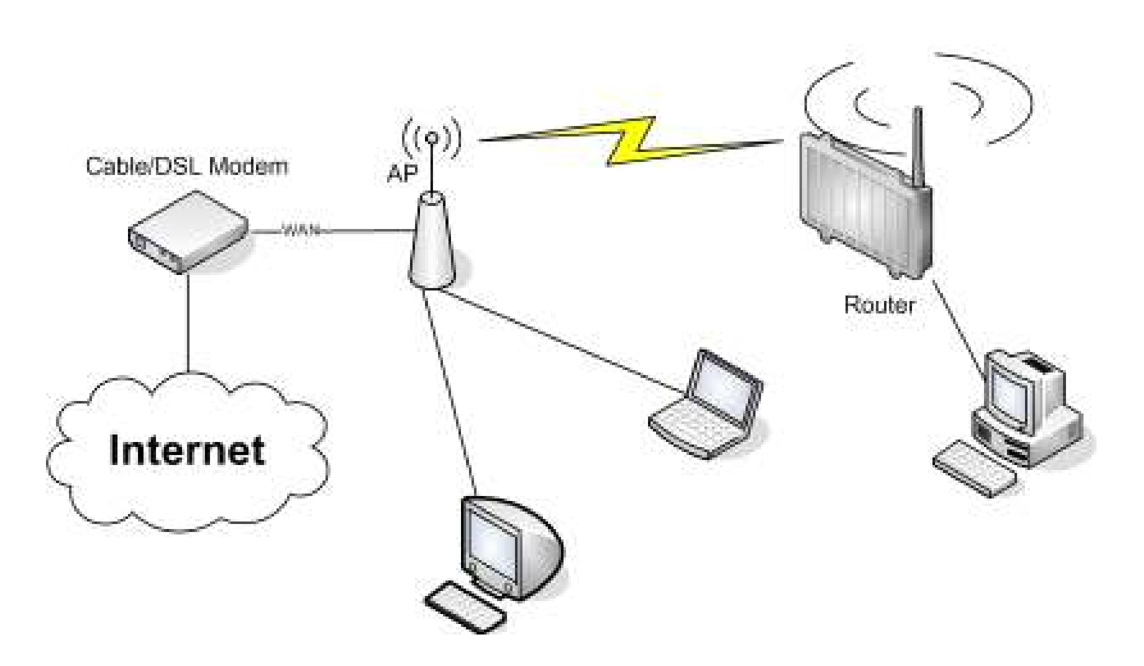
- Wählen und Konfigurieren Sie den Sicherheitsmodus analog zu den Einstellungen des Access Points
- Klicken Sie auf „Apply Settings“

Prüfen Sie nach dem Neustart des Routers, ob dieser als Wireless Client auf dem Access Point angezeigt wird bzw. ob der als Client konfigurierte Router sich mit dem Access Point verbindet. Wenn das WAN Interface des Routers auf DHCP konfiguriert wurde, sollte der Router entsprechend eine IP-Adresse zugewiesen bekommen.

Sie können nun entweder Geräte per LAN anschließen oder aber ein weitere Wireless Interface als Access Point konfigurieren um Wireless Clients mit dem Router zu verbinden.

3.3. Wireless Client Bridge

Eine Wireless Brigde kann verwendet werden, um einen weiteren Access Point transparent in das interne LAN eines anderen Access Points einzubinden. Über das LAN oder ein weiteres WLAN-Interface angebundene Clients sind dann direkt an das interne LAN des Access Points angebunden. Das WAN-Interface wird bei dieser Konfiguration nicht benötigt und kann deaktivert werden.



Setup -> Basic Setup

- *WAN Setup*
  - Stellen Sie den „Connection Type“ auf „Disabled“
- *Network Setup*
  - Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - Setzen Sie „DHCP Server“ auf „Disable“
- *Time Settings*
  - Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „Client Bridge“
- Stellen Sie bei „Wireless Network Mode“ den Modus des Access Points ein, mit dem sich der Router verbinden soll
- Setzen Sie die „Wireless Network Name (SSID)“ auf den für den Access Point konfigurierten Netzwerknamen
- Klicken Sie auf „Save“

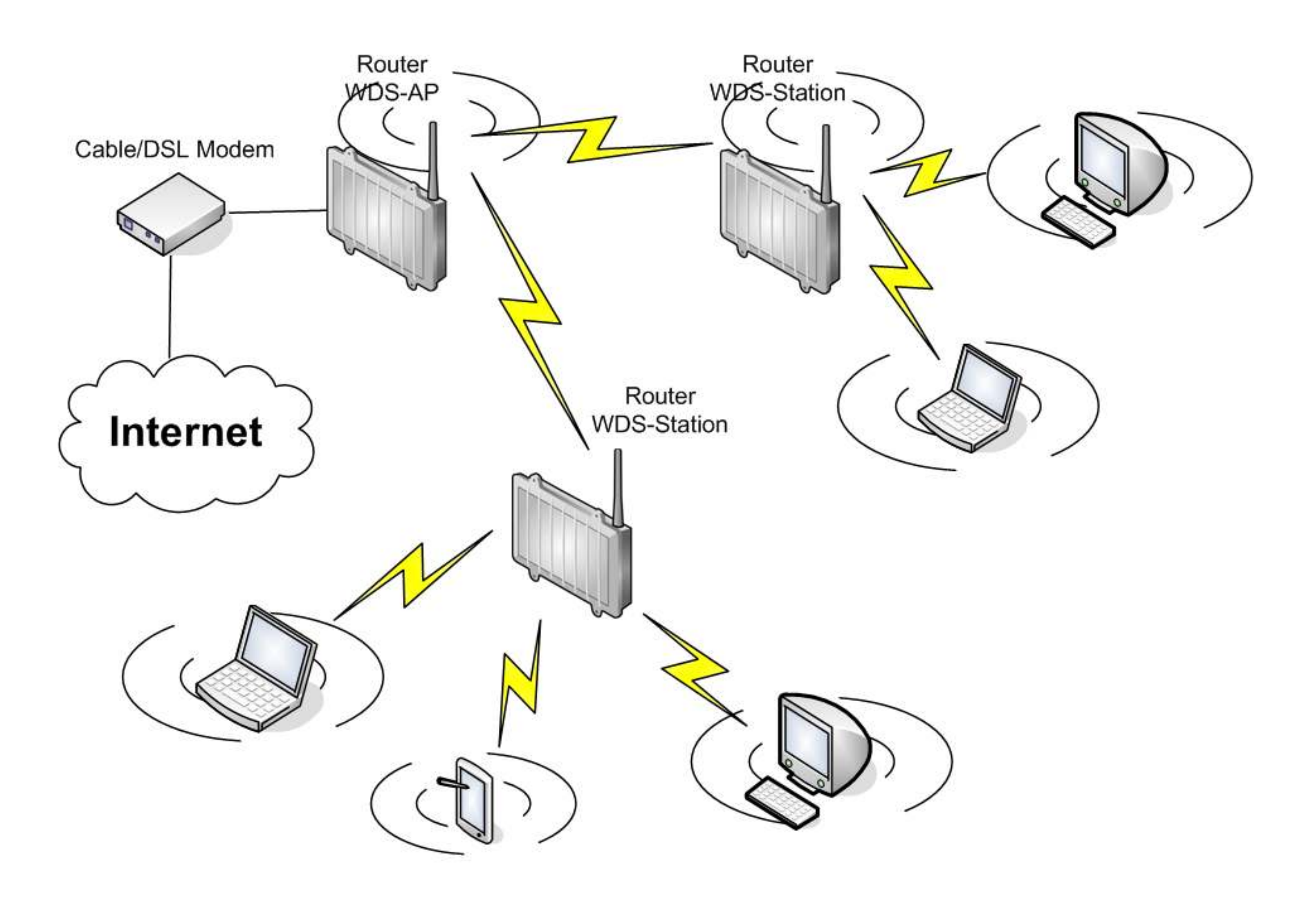
Wireless -> Wireless Security

- Wählen und konfigurieren Sie den Sicherheitsmodus analog zu den Einstellungen des Access Points
- Klicken Sie auf „Apply Settings“

Prüfen Sie nach dem Neustart des Routers, ob dieser als Wireless Client auf dem Access Point angezeigt wird bzw. ob der als Client Bridge konfigurierte Router sich mit dem Access Point verbindet. Wenn das WAN Interface des Routers auf DHCP koniguriert wurde, sollte der Router entsprechend eine IP-Adresse zugewiesen bekommen.

3.4. WDS AP & WDS Station

Neben den Modi AP und Client stehen die auf den ersten Blick identischen Modi WDS AP und WDS Station zur Verfügung. Ähnlich wie bei AP und Client verbindet sich die WDS Station ähnlich einem Client mit dem WDS AP. Allerdings erlaubt der Modus WDS Station WLAN Clients sich mit dieser ähnlich einem AP zu verbinden. Dadurch kann die Abdeckung des Netzes erweitert werden, ohne ein weiteres WLAN Interface zu benötigen. Im Gegensatz zu vielen WDS Implementierungen kann der Datenverkehr zwischen einem WDS AP und den WDS Stations auch mit WPA2 verschlüsselt werden.



3.4.1. WDS AP

Setup -> Basic Setup

- *WAN Setup*
  - Wählen Sie bei „Connection Type“ die Art der WAN-Anbindung und nehmen Sie die jeweiligen Einstellungen vor
- *Network Setup*
  - Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - Setzen Sie „DHCP Type“ auf „DHCP Server“ (sofern nicht gesetzt)
  - Setzen Sie „DHCP Server“ auf „Enable“ (sofern nicht gesetzt)
  - Passen Sie ggf. den DHCP-Adressbereich an, den der Server vergeben soll
- *Time Settings*
  - Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „WDS AP“
- Stellen Sie bei „Wireless Network Mode“ den gewünschten Modus ein, beachten Sie, dass der gemischte Betrieb (BG-Mixed) von 802.11b und 802.11g (2,4 GHz) zu Performanceeinbußen führt

- Setzen Sie die „Wireless Network Name (SSID)“ auf den gewünschten Netzwerknamen
- Klicken Sie auf „Save“

Wireless -> Wireless Security

- Wählen und konfigurieren Sie den gewünschten Sicherheitsmodus (beachten Sie, dass WEP konzeptionell unsicher ist und nur verwendet werden sollte, wenn dies absolut unabdingbar ist)
- Klicken Sie auf „Apply Settings“

Sie können nun den Router über das LAN-Interface mit dem Internet / Ihrem Netzwerk verbinden. Wenn Sie WDS Stations mit dem WDS AP verbinden, sollten diese nach erfolgreichem Verbindungsaufbau im Statusbereich aufgeführt werden.

3.4.2. WDS Station

Setup -> Basic Setup

- *WAN Setup*
  - o Stellen Sie bei „Connection Type“ entweder „Static IP“ (falls auf der Seite des AP kein DHCP Server läuft) oder „DHCP“ ein
- *Network Setup*
  - o Setzen Sie bei „Router IP“ die gewünschte IP-Adresse des Routers im LAN
  - o Setzen Sie „DHCP Server“ auf „Disable“
  - o Passen Sie ggf. den DHCP-Adressbereich an, den der Server vergeben soll *Time Settings*
- *Time Settings*
  - o Stellen Sie hier die erforderlichen Werte für Ihre Zeitzone ein (optional)
- Klicken Sie auf „Save“

Wireless -> Basic Settings

- Setzen Sie „Regulatory Domain“ auf das Land, in dem der Router betrieben werden soll
- Tragen Sie bei „Antenna Gain“ den Antennengewinn der verwendeten Antenne ein, das System passt die Sendeleistung anhand der „Regulatory Domain“ entsprechend an. Beachten Sie, dass lange HF-Kabel das Signal dämpfen, berücksichtigen Sie dies ggf. beim Antennengewinn.
- Setzen Sie den „Wireless Mode“ auf „WDS Station“
- Stellen Sie bei „Wireless Network Mode“ den Modus des Access Points ein, mit dem sich der Router verbinden soll
- Setzen Sie die „Wireless Network Name (SSID)“ auf den für den Access Point konfigurierten Netzwerknamen
- Klicken Sie auf „Save“

Wireless -> Wireless Security

- Wählen und Konfigurieren Sie den Sicherheitsmodus analog zu den Einstellungen des Access Points
- Klicken Sie auf „Apply Settings“

Prüfen Sie nach dem Neustart des Routers, ob dieser als WDS Station auf dem WDS AP angezeigt wird bzw. ob die WDS Station sich mit dem WDS AP verbindet.

4. Lizenzinformationen

Die Firmware, die in diesem Produkt verwendet wird, beinhaltet Software, die der GNU Public Licenz (GPL) bzw. der GNU Lesser Public License (LGPL) unterliegt. Soweit im Rahmen der GPL und der LGPL anwendbar sind die Bedingungen der GPL und der LGPL sowie die diesbezüglichen Quellcodes vom Hersteller verfügbar. Der der GPL bzw. der LGPL unterliegende Code der Software wird bereitgestellt, ohne dass sich daraus Gewährleistungs- oder Haftungsansprüche ableiten lassen. Weitere Details entnehmen Sie bitte den Bedingung der GPL bzw. der LGPL.

4.1. GNU General Public License

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

4.1.1. Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

4.1.2. GNU General Public License – Terms and Conditions or Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on

the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

4.1.3. NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.